UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

IN RE: AVIS RENT A CAR SYSTEM, LLC SECURITY INCIDENT LITIGATION	**Case No. 2:24-cv-09243** **CONSOLIDATED CLASS ACTION** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Brooke Pestano, Jason Shay, Chase Schachenman, Jason Bundrick, Bill D. Thomas, Tanisorn Tatiyaratana, Michael Beauchane, Joe Lopez, Katrina Robertson, and Brian Harris ("Plaintiffs"), on behalf of themselves and all others similarly situated, bring this Consolidated Class Action Complaint ("Complaint"), against Defendants Avis Rent A Car System, LLC and Avis Budget Group, Inc. (collectively, "Avis" or "Defendants") for failure to properly secure and safeguard Plaintiffs' and "Class members'" (defined below) highly sensitive personal information stored within Defendants' information network, and allege as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which is based on personal knowledge:

NATURE OF THE CASE

1. Plaintiffs bring this class action against Avis for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Avis customers' highly valuable, protected personally identifiable information, including, *inter alia*, customers' full names, driver's license information, credit card numbers and expiration dates, dates of birth, and phone numbers (collectively "PII" or "Private Information") from hackers, as well as for Avis's failure to comply with industry standards to protect information systems that contain customer PII.

2. Entities that provide services and handle consumers' sensitive PII owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII to unauthorized persons—especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private financial matters.

3. The harm resulting from a breach of private data manifests in several ways, including identity theft and financial fraud. The exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time, energy and money to closely monitor their credit, financial accounts, health records, and email accounts, and to take a number of additional prophylactic measures.

4. As discussed in more detail below, Avis breached its duty to protect the sensitive PII entrusted to it. As such, Plaintiffs bring this class action on behalf of themselves and the approximately 300,000 other individuals whose PII was accessed and exposed to unauthorized third parties during a data breach of Defendants' system between August 3, 2024 and August 6, 2024, which Avis discovered on August 5, 2024, and announced publicly via letter to affected individuals on or about September 4, 2024 (the "Data Breach").

5. Avis is a rental car service company that operates in approximately 5,500 locations in more than 165 countries and serves hundreds of thousands of customers nationwide.[1]

6. To provide its car rental services, Avis requests and obtains customers' sensitive

[1] *Avis Corporate Facts*, https://www.avis.com/en/about-avis/company-information/corporate-facts (last visited Dec. 20, 2024).

PII. As Avis is or should have been aware, this type of personal and sensitive data is highly targeted by hackers who seek to exploit that data for nefarious purposes. In the wrong hands, the sensitive data may be wielded to cause significant harm to the individuals to whom the data relates.

7. Because Avis knowingly collects and stores its customers' PII, Avis, in turn, has a resulting duty to secure, maintain, protect, and safeguard the PII with which it has been entrusted against unauthorized access and exfiltration through reasonable, adequate, and standard data security measures.

8. Avis expressly recognizes this duty; for instance, Avis's Privacy Notice ("Privacy Notice") assures its customers that "[t]he security of personal information is important to us."[2]

9. Despite Avis's duty to safeguard its customers' PII, Plaintiffs' and Class members' sensitive information was exposed to unauthorized third parties during a data breach of Defendants' business applications that occurred between August 3, 2024 and August 6, 2024, resulting in the unauthorized access and exfiltration of the PII of approximately 300,000 of Defendants' current and former customers.[3]

10. As a direct and proximate result of Defendants' failure to implement and follow basic, standard security procedures, Plaintiffs' and Class members' PII is now in the hands of cybercriminals. Plaintiffs' and Class members' PII has been accessed by hackers, posted on the dark web, and exposed to an untold number of unauthorized individuals.

11. On or about September 4, 2024, Avis began sending data breach letters ("Notice Letter") to individuals whose information was compromised because of the hacking incident.[4]

---

[2] *Privacy Notice*, Avis, https://www.avis.com/en/legal-documents/privacy-notice (last visited Dec. 20, 2024).
[3] *Id.*
[4] *Avis Notice Letter to Customers*, attached as Exhibit A.

12. On or about September 5, 2024, Avis filed an official notice of a hacking incident with the Offices of the Attorney General in both Maine and California.[5]

13. According to Avis's report to the Office of the Attorney General in Maine, approximately 299,006 individuals have been affected by the Data Breach. [6]

14. Plaintiffs and Class members were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

15. Plaintiffs, on behalf of themselves and others similarly situated, bring claims for negligence, negligence *per se*, breach of contract, breach of an implied contract, breach of fiduciary duty, breach of confidence, intrusion upon seclusion/invasion of privacy, unjust enrichment, violations of various state consumer protection statutes, including the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq.*, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

16. To recover from Defendants for their sustained, ongoing, and future harms, Plaintiffs seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendants to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendants; and 3) provide, at their own expense, all impacted victims with lifetime identity theft protection services.

---

[5] *Avis Notice Letter*, available at: https://www.maine.gov/cgi-bin/agviewerad/ret?loc=1225 (last visited Dec. 20, 2024).
[6] *Id.*

PARTIES

Plaintiffs

Plaintiff Brooke Pestano

17. Plaintiff Brooke Pestano is an adult individual and, at all relevant times herein, a resident and citizen of the state of Florida, residing in Palm Bay, Florida. Plaintiff Pestano is a victim of the Data Breach.

18. Prior to August 2024, Plaintiff Pestano was an Avis customer and was required to provide her Private Information.

19. In October 2024, Plaintiff Pestano received a Notice letter dated September 4, 2024, which told her that her Private Information had been obtained during the Data Breach. The notice letter informed her that the Private Information compromised included her name, driver's license, credit card number and expiration date, date of birth, and phone number.

Plaintiff Jason Shay

20. Plaintiff Jason Shay is an adult individual and, at all relevant times herein, a resident and citizen of the state of Texas, residing in McKinney, Texas. Plaintiff Shay is a victim of the Data Breach.

21. Prior to August 2024, Plaintiff Shay was an Avis customer and was required to provide his Private Information.

22. On or about September 4, 2024, Plaintiff Shay was notified of the Data Breach and the impact to his PII via letter from Defendants.

Plaintiff Chase Schachenman

23. Plaintiff Chase Schachenman is an adult individual and, at all relevant times herein, a resident and citizen of the state of Minnesota, residing in Saint Paul, Minnesota. Plaintiff Schachenman is a victim of the Data Breach.

24. Prior to August 2024, Plaintiff Schachenman used Defendants' rental car service and was required to provide his Private Information.

25. Plaintiff Schachenman received a Data Breach notification letter from Avis dated September 4, 2024, concerning this Data Breach and the impact to his PII.

Plaintiff Jason Bundrick

26. Plaintiff Jason Bundrick is an adult individual and, at all relevant times herein, a resident and citizen of the state of South Carolina, residing in West Columbia, South Carolina. Plaintiff Bundrick is a victim of the Data Breach.

27. Prior to August 2024, Plaintiff Bundrick used Defendants' rental car service and was required to provide his Private Information.

28. Plaintiff Bundrick received a data breach notification letter from Avis dated September 4, 2024, concerning this Data Breach and the impact to his PII.

Plaintiff Bill R. Thomas

29. Plaintiff Bill R. Thomas is an adult individual and, at all relevant times herein, a resident and citizen of the state of Oklahoma, residing in Oklahoma City, Oklahoma. Plaintiff Thomas is a victim of the Data Breach.

30. Plaintiff Thomas is a long-time, repeat customer of Avis, and was required to provide his Private Information.

31. Plaintiff Thomas recently received a Notice letter from Avis dated September 4, 2024, notifying him of the Data Breach and the impact to his PII.

Plaintiff Tanisorn Tatiyaratana

32. Plaintiff Tanisorn Tatiyaratana is an adult individual and, at all relevant times herein, a resident and citizen of the state of Illinois, residing in Chicago, Illinois. Plaintiff

Tatiyaratana is a victim of the Data Breach.

33. Prior to August 2024, Plaintiff Tatiyaratana was required to provide his Private Information to Avis when renting a car from Defendants.

34. Plaintiff Tatiyaratana received a letter notice from Avis dated September 4, 2024, notifying him that his Private Information was improperly exposed to unauthorized third parties. This Private Information included Plaintiff's name, driver's license number, credit card number and expiration date, date of birth, and phone number.

Plaintiff Michael Beauchane

35. Plaintiff Michael Beauchane is an adult individual and, at all relevant times herein, a resident and citizen of the state of Tennessee, residing in Greenbrier, Tennessee. Plaintiff Beauchane is a victim of the Data Breach.

36. Plaintiff Beauchane is a former Avis customer, who rented vehicle(s) from it from on or around June 2019 through on or around July 14, 2019. He was required to provide his Private Information to Avis when renting cars from Defendants.

37. Plaintiff Beauchane received a copy of the breach notice notifying him that his Private Information was improperly exposed to unauthorized third parties.

Plaintiff Joe Lopez

38. Plaintiff Joe Lopez is an adult individual and, at all relevant times herein, a resident and citizen of the state of California, residing in Los Angeles, California. Plaintiff Lopez is a victim of the Data Breach.

39. Plaintiff Lopez is a long-time, repeat customer of Avis and was required to provide it with substantial amounts of his Private Information.

40. On or about September 17, 2024, Plaintiff Lopez received a letter entitled "Notice

of Data Breach" which told him that his Private Information had been obtained during the Data Breach. The notice letter informed him that the compromised Private Information included his name, driver's license, credit card number and expiration date, date of birth, and phone number.

Plaintiff Katrina Robertson

41. Plaintiff Katrina Robertson is an adult individual and, at all relevant times herein, a resident and citizen of the state of Kansas, residing in Merriam, Kansas. Plaintiff Robertson is a victim of the Data Breach.

42. Prior to August 2024, Plaintiff Robertson was an Avis customer and was required to provide her Private Information.

43. Subsequent to September 4, 2024, Plaintiff Robertson became aware that her Private Information was improperly exposed to unauthorized third parties as part of the Data Breach.

Plaintiff Brian Harris

44. Plaintiff Brian Harris is an adult individual and, at all relevant times herein, a resident and citizen of the state of California, residing in Lawndale, California. Plaintiff Harris is a victim of the Data Breach.

45. Plaintiff Harris is a long-time, repeat customer of Avis and was required to provide his Private Information.

46. Subsequent to September 4, 2024, Plaintiff Harris received a Notice letter and became aware that his Private Information was improperly exposed to unauthorized third parties as part of the Data Breach.

Defendants Avis Rent A Car System, LLC and Avis Budget Group, Inc.

47. Upon information and belief: the sole member of Defendant Avis Rent A Car

System, LLC is Avis Group Holdings, LLC ("AGH"); AGH is a Delaware limited liability company with its principal place of business at 6 Sylvan Way, Parsippany, New Jersey; the sole member of AGH is Avis Car Rental Group, LLC ("ACRG"); ACRG is a Delaware limited liability company with its principal place of business at 6 Sylvan Way, Parsippany, New Jersey; The sole member of ACRG is Avis Budget Car Rental, LLC ("ABCR"); ABCR is a Delaware limited liability company with its principal place of business at 6 Sylvan Way, Parsippany, New Jersey; the sole member of ABCR is Avis Budget Holdings, LLC ("ABH"); ABH is a Delaware limited liability company with its principal place of business at 6 Sylvan Way, Parsippany, New Jersey; the sole member of ABH was Cendant Finance Holding Company LLC ("CFHC") until its voluntary dissolution in 2018; CFHC was, prior to dissolution, a Delaware limited liability company with its principal place of business at 6 Sylvan Way, Parsippany, New Jersey; and the sole member of CFHC was Avis Budget Group, Inc. ("ABG"); ABG is a Delaware corporation with its principal place of business at 6 Sylvan Way, Parsippany, New Jersey. As a result, Defendant Avis Rent A Car LLC is a citizen of the State of New Jersey. Defendant Avis Budget Group, Inc. is a corporate citizen of the State of New Jersey, with its headquarters at 379 Interpace Parkway, Parsippany, New Jersey 07054. ABG is the parent company of Defendant Avis Rent A Car System LLC.

48. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs.

49. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

JURISDICTION AND VENUE

50. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members, including Plaintiffs herein, who are citizens of states other than Defendants' state of citizenship.

51. This Court has personal jurisdiction over the parties in this case. Defendant Avis conducts business in this District and is a citizen of this District by virtue of having its principal place of business located in this District.

52. Venue is proper in this District under 28 U.S.C. §1391(b) because Avis is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL BACKGROUND

A. Avis and the Services it Provides.

53. Avis is part of Avis Budget Group, Inc., a car rental agency holding company based in Parsippany, New Jersey. Avis operates at approximately 5,500 locations in more than 165 countries.[7]

54. Since its founding in 1946, Avis has grown into one of the largest and most ubiquitous car rental companies in the United States.[8]

55. Avis rents cars and offers related products, services, and protections, such as GPS navigation accessories, mobile applications, roadside assistance, and various rental insurance options.[9]

---

[7] *Avis Corporate Facts, supra* note 1.
[8] *Avis History*, Avis, https://www.avis.com/en/about-avis/company-information/historical-chronology (last visited Dec. 20, 2024).
[9] *Products and Services*, Avis, https://www.avis.com/en/products-and-services (last visited Dec. 20, 2024).

56. To conduct its car rental business, Avis receives and handles PII, which includes, *inter alia*, consumers' full name, address, phone number, date of birth, driver's license number and credit card information.

57. Avis uses this information for, *inter alia*, marketing, advertising, and business operations.

58. Customers, such as Plaintiffs and Class members, *must* provide this information in order to receive Avis's services: Avis informs its customers, "If you do not provide the information we request, we may not be able to provide our products or services to you."[10]

59. In its Privacy Policy, Avis lists the non-public information it collects from its customers, including the following:

> [Y]our name and contact information, birthdate, government identification, payment information, membership ID, program ID, whether you are a part of a corporate or rewards program, payment arrangements, insurance arrangements, and information related to your rentals or use of products or services we provide or enable.[11]

60. Plaintiffs entrusted this information to Avis with the reasonable expectation and mutual understanding that Avis would comply with its obligations to keep such information confidential and secure from unauthorized access.

61. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' PII, Avis assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class members' PII from unauthorized access, compromise, and exfiltration.

62. Avis expressly recognizes these duties, representing that, "The security of personal information is important to us. We take reasonable steps designed to protect personal information

[10] *Privacy Notice*, *supra* note 2.
[11] *Id.*

from unauthorized use, access, disclosure, alteration, destruction or loss."[12] Furthermore, Avis states:

> To determine the appropriate duration of the retention of personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of personal information, and whether we can attain our objectives by other means, as well as our legal, regulatory, tax, accounting, and other applicable obligations.[13]

63. Plaintiffs and Class members had a reasonable expectation, based in part on Avis's own statements, that their PII would be protected. However, despite its stated commitment to data security, Avis failed to adopt reasonable data security measures to prevent unauthorized access to Plaintiffs' and Class members' PII and allowed for the access to and the exfiltration of said information by unauthorized bad actors.

64. Had Avis maintained its data security network and worked diligently to correct vulnerabilities, remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Avis could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class members' confidential PII.

65. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including payments made by or on behalf of Plaintiffs and Class members to Avis.

B. Avis Knew the Risks of Storing Valuable PII and the Foreseeable Harm to its Customers.

66. At all relevant times, Avis knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

---

[12] *Id.*
[13] *Id.*

67. As set forth above, Avis explicitly acknowledges that security of personal information is important, and promises that it will take reasonable steps to protect personal information from unauthorized use, access, disclosure, alteration, destruction or loss.[14]

68. Avis also knew or should have known that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

69. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2019, 2.5 million people reported some form of identity theft or fraud compared to 4.4 million people in 2021.[15]

70. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

71. PII is a valuable property right.[16] The value of PII as a commodity is measurable.[17] "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

[14] *See Privacy Notice*, *supra* note 2.

[15] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited December 20, 2024).

[16] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

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

frameworks."[18] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[19] 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.

72. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, 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 aggregated, and becomes more valuable to thieves and more damaging to victims.

73. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[20]

74. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these

---

[18] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[19] *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*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[20] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 17, 2023).

forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

75. 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."[21]

76. 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.

77. Based on the value of its customers' PII to cybercriminals and cybercriminals' propensity to target large companies, Avis certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Avis Breached its Duty to Protect its Customers' PII.

78. On or about September 4, 2024, Avis announced that it experienced a security incident disrupting access to its systems.

79. As part of this security incident, Avis customers' PII was accessed and exposed to unauthorized third parties.

80. As noted above, the consumer PII compromised in this Data Breach includes dates of birth, driver's license and credit card information and addresses.

81. On September 5, 2024, Avis reported to the Offices of the Attorneys General of

[21] 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.guanotronic.com/~serge/papers/weis07.pdf.

Maine and California that it had been affected by a data breach. In its report to Maine, Avis indicated that the breach was related to "insider wrongdoing," though this statement is not further explained.[22]

82. In the Notice Letters, Avis described the circumstances surrounding the Data Breach as follows:

> We discovered on August 5, 2024, that an unauthorized third party gained access to one of our business applications. After becoming aware of the incident, we immediately took steps to end the unauthorized access, began an investigation with assistance from cybersecurity experts, and alerted the relevant authorities. Based on our investigation, we determined that the unauthorized access occurred between August 3, 2024, and August 6, 2024.[23]

83. Like Plaintiffs, other potential Class members received similar notices informing them that their PII was exposed in the Data Breach.

84. All in all, approximately 300,000 individuals with information stored on Avis's system had their PII breached.

85. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic security procedures to protect their customers' PII, including their failure to diligently monitor and patch vulnerabilities in their network, and their failure to follow industry guidelines and implement security measures recommended by data security experts.

D. Plaintiffs' Experiences as a Result of the Data Breach.

Plaintiff Brooke Pestano's Experience and Injuries

86. Upon information and belief, prior to the August 2024 Data Breach, Avis

---

[22] *Data Breach Notification*, Office of the Maine Attorney General (Sept. 5, 2024), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ccfece24-0b9c-4251-a89b-0fd68ecbda12.html; *Data Breach Notification*, Office of the California Attorney General (Sept. 5, 2024). https://oag.ca.gov/ecrime/databreach/reports/sb24-591235.

[23] *Notice Letter*, *supra* notes 4, 5.

maintained Plaintiff Brooke Pestano's PII in its system.

87. When Plaintiff Pestano first became a customer she provided her PII to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continue to maintain Plaintiff Pestano's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

88. Plaintiff Pestano reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

89. On information and belief, Plaintiff Pestano's PII was accessed and stolen in the Data Breach and has already been published by cybercriminals on the Dark Web, including her Social Security number.

90. After the Data Breach, Plaintiff Pestano became aware of multiple attempts by an unknown third party to open credit accounts in her name and other fraudulent activity on her financial accounts.

91. In fact, Plaintiff Pestano attempted to establish a new line of credit but her application was declined.

92. Additionally, after the Data Breach, she is experiencing a significant increase in spam calls, texts and emails and is required to expend time attempting to block most of those.

93. Plaintiff Pestano has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Avis directed Plaintiff Pestano to take those steps in its Notice Letter.

94. Because of Defendants' Data Breach, Plaintiff Pestano has suffered—and will continue to suffer—from anxiety, sleep disruption, stress, fear, and frustration. Such injuries go

far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Pestano's injuries are precisely the type of injuries that the law contemplates and addresses.

95. Plaintiff Pestano suffered actual injury from the exposure and theft of her PII—which violates her rights to privacy.

96. Plaintiff Pestano suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

97. Because of the Data Breach, Plaintiff Pestano anticipates spending considerable amounts of time and money to try and mitigate her injuries.

98. Today, Plaintiff Pestano has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Plaintiff Jason Shay's Experience and Injuries

99. Upon information and belief, prior to the August 2024 Data Breach, Avis maintained Plaintiff Shay's PII in its system.

100. Plaintiff Shay provided his PII to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continue to maintain Plaintiff Shay's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

101. Plaintiff Shay reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

102. On information and belief, Plaintiff Shay's PII was accessed and stolen in the Data Breach. Further, Plaintiff Shay is aware that his PII has already been published by cybercriminals

on the Dark Web.

103. Since the Data Breach, Plaintiff Shay has experienced an increase in spam emails, spam social media direct messages, suspicious (*i.e.*, phishing scam) phone calls and texts.

104. Plaintiff Shay has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Avis directed Plaintiff Shay to take those steps in its Notice Letter.

105. Because of Defendants' Data Breach, Plaintiff Shay has suffered—and will continue to suffer —from emotional distress. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Shay's injuries are precisely the type of injuries that the law contemplates and addresses.

106. Plaintiff Shay suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

107. Plaintiff Shay suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

108. Plaintiff Shay suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff Shay's PII right in the hands of criminals.

109. Because of the Data Breach, Plaintiff Shay anticipates spending considerable amounts of time and money to try and mitigate his injuries.

110. Today, Plaintiff Shay has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Plaintiff Chase Schachenman's Experience and Injuries

111. Upon information and belief, prior to the August 2024 Data Breach, Avis maintained Plaintiff Schachenman's PII in its system.

112. Plaintiff Schachenman provided his PII to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continue to maintain Plaintiff Schachenman's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

113. Plaintiff Schachenman reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

114. On information and belief, Plaintiff Schachenman's PII was accessed and stolen in the Data Breach. Further, Plaintiff is aware that his PII has already been published by cybercriminals on the Dark Web, including his full name, Social Security number, past driver's license information, and credit card numbers.

115. Since the Data Breach, Plaintiff Schachenman has experienced an increase in spam emails, spam social media direct messages, scam phone calls and texts.

116. Plaintiff Schachenman has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Avis directed Plaintiff Schachenman to take those steps in its Notice Letter.

117. Because of Defendants' Data Breach, Plaintiff Schachenman has suffered—and will continue to suffer —from anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Schachenman's injuries are precisely the type of injuries that the law contemplates and addresses.

118. Plaintiff Schachenman suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

119. Plaintiff Schachenman suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

120. Plaintiff Schachenman suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff Schachenman's PII right in the hands of criminals.

121. Because of the Data Breach, Plaintiff Schachenman anticipates spending considerable amounts of time and money to try and mitigate his injuries.

122. Today, Plaintiff Schachenman has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Plaintiff Jason Bundrick's Experience and Injuries

123. Upon information and belief, prior to the August 2024 Data Breach, Avis maintained Plaintiff Bundrick's PII in its system.

124. Plaintiff Bundrick provided his PII to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continue to maintain Plaintiff Bundrick's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

125. Plaintiff Bundrick reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

126. On information and belief, Plaintiff Bundrick's PII was accessed and stolen in the

Data Breach and has already been published—or will be published imminently—by cybercriminals on the Dark Web.

127. Prior to the Data Breach, Plaintiff Bundrick was very careful about sharing his sensitive PII in order to protect his privacy and security. He always used unique passwords for important accounts and regularly checked his credit and banking accounts.

128. Since the Data Breach, Plaintiff Bundrick has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Avis directed Plaintiff Bundrick to take those steps in its Notice Letter.

129. Plaintiff Bundrick fears for his personal financial security and worries about what information was exposed in the Data Breach.

130. Because of Defendants' Data Breach, Plaintiff Bundrick has suffered—and will continue to suffer —from anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Bundrick's injuries are precisely the type of injuries that the law contemplates and addresses.

131. Plaintiff Bundrick suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

132. Plaintiff Bundrick suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

133. Plaintiff Bundrick suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff Bundrick's PII right in the hands of criminals.

134. Because of the Data Breach, Plaintiff Bundrick anticipates spending considerable

amounts of time and money to try and mitigate his injuries.

135. Today, Plaintiff Bundrick has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Plaintiff Bill Thomas's Experience and Injuries

136. Upon information and belief, prior to the August 2024 Data Breach, Avis maintained Plaintiff Thomas's PII in its system.

137. Plaintiff Thomas provided his PII to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continue to maintain Plaintiff Thomas's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

138. Plaintiff Thomas reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

139. On information and belief, Plaintiff Thomas's PII was accessed and stolen in the Data Breach and has already been published by cybercriminals on the Dark Web.

140. Since the Data Breach, Plaintiff Thomas has experienced a spike in spam emails, texts and scam phone calls. He has received multiple "click on this to change your password" scam emails.

141. Plaintiff Thomas has also noted multiple fraudulent charges on his credit card accounts. There were repeated incidents of fraudulent charges on his Capital One credit card, an attempted theft of funds from his PayPal account that was only prevented by a notice sent to him by his bank, and multiple fraudulent attempts to request funds and obtain login info from his other on-line financial accounts.

142. Plaintiff Thomas fears for his personal financial security and worries about what information was exposed in the Data Breach.

143. Because of Defendants' Data Breach, Plaintiff Thomas has suffered—and will continue to suffer —from anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Thomas's injuries are precisely the type of injuries that the law contemplates and addresses.

144. Plaintiff Thomas suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

145. Plaintiff Thomas suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

146. Plaintiff Thomas suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff Thomas's PII right in the hands of criminals.

147. Because of the Data Breach, Plaintiff Thomas anticipates spending considerable amounts of time and money to try and mitigate his injuries.

148. Today, Plaintiff Thomas has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Plaintiff Tanisorn Tatiyaratana's Experience and Injuries

149. Upon information and belief, prior to the August 2024 Data Breach, Avis maintained Plaintiff Tatiyaratana's PII in its system.

150. Plaintiff Tatiyaratana provided his PII to Defendants and trusted the company

would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continue to maintain Plaintiff Tatiyaratana's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

151. Plaintiff Tatiyaratana reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

152. On information and belief, Plaintiff Tatiyaratana's PII was accessed and stolen in the Data Breach and has already been published—or will be published imminently—by cybercriminals on the Dark Web.

153. Plaintiff Tatiyaratana has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Avis directed Plaintiff Tatiyaratana to take those steps in its Notice Letter.

154. In the aftermath of the Data Breach, Plaintiff Tatiyaratana has suffered from a spike in spam and scam phone calls.

155. Plaintiff Tatiyaratana fears for his personal financial security and worries about what information was exposed in the Data Breach.

156. Because of Defendants' Data Breach, Plaintiff Tatiyaratana has suffered—and will continue to suffer —from anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Tatiyaratana's injuries are precisely the type of injuries that the law contemplates and addresses.

157. Plaintiff Tatiyaratana suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

158. Plaintiff Tatiyaratana suffered actual injury in the form of damages to and

diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

159. Plaintiff Tatiyaratana suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff Tatiyaratana's PII right in the hands of criminals.

160. Because of the Data Breach, Plaintiff Tatiyaratana anticipates spending considerable amounts of time and money to try and mitigate his injuries.

161. Today, Plaintiff Tatiyaratana has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Plaintiff Michael Beauchane's Experience and Injuries

162. Upon information and belief, prior to the August 2024 Data Breach, Avis maintained Plaintiff Beauchane's PII in its system.

163. Plaintiff Beauchane provided his PII to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continue to maintain Plaintiff Beauchane's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

164. Plaintiff Beauchane reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

165. On information and belief, Plaintiff Beauchane's PII was accessed and stolen in the Data Breach and has already been published by cybercriminals on the Dark Web. Plaintiff Beauchane has received notice that his name, Social Security number, email address and driver's license number have been exposed.

166. Since the Data Breach, Plaintiff Beauchane has suffered from a spike in spam and scam phone calls.

167. Plaintiff Beauchane has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Avis directed Plaintiff to take those steps in its Notice Letter.

168. Plaintiff Beauchane fears for his personal financial security and worries about what information was exposed in the Data Breach.

169. Because of Defendants' Data Breach, Plaintiff Beauchane has suffered—and will continue to suffer —from anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Beauchane's injuries are precisely the type of injuries that the law contemplates and addresses.

170. Plaintiff Beauchane suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

171. Plaintiff Beauchane suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

172. Plaintiff Beauchane suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff Beauchane's PII right in the hands of criminals.

173. Because of the Data Breach, Plaintiff Beauchane anticipates spending considerable amounts of time and money to try and mitigate his injuries.

174. Today, Plaintiff Beauchane has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendants' possession—is protected

and safeguarded from additional breaches.

Plaintiff Joe Lopez's Experience and Injuries

175. Upon information and belief, prior to the August 2024 Data Breach, Avis maintained Plaintiff Lopez's PII in its system.

176. Plaintiff Lopez provided his PII to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continue to maintain Plaintiff Lopez's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

177. Plaintiff Lopez reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

178. On information and belief, Plaintiff Lopez's PII was accessed and stolen in the Data Breach and has already been published—or will be published imminently—by cybercriminals on the Dark Web.

179. Since the Data Breach, during November 2024, Plaintiff Lopez received a notice that there was an unauthorized charge on his Amazon.com account. Since then, he has been required to cancel and obtain a new credit card.

180. Plaintiff Lopez has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Avis directed Plaintiff Lopez to take those steps in its Notice Letter.

181. Further, in the aftermath of the Data Breach, Plaintiff Lopez suffered from a spike in spam and scam phone calls.

182. Plaintiff Lopez fears for his personal financial security and worries about what information was exposed in the Data Breach.

183. Because of Defendants' Data Breach, Plaintiff Lopez has suffered—and will continue to suffer —from anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Lopez's injuries are precisely the type of injuries that the law contemplates and addresses.

184. Plaintiff Lopez suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

185. Plaintiff Lopez suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

186. Plaintiff Lopez suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff's PII right in the hands of criminals.

187. Because of the Data Breach, Plaintiff Lopez anticipates spending considerable amounts of time and money to try and mitigate his injuries.

188. Today, Plaintiff Lopez has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Plaintiff Katrina Robertson's Experience and Injuries

189. Upon information and belief, prior to the August 2024 Data Breach, Avis maintained Plaintiff Katrina Robertson's PII in its system.

190. On information and belief, Plaintiff Robertson's PII was accessed and stolen in the Data Breach and has already been published by cybercriminals on the Dark Web.

191. Prior to the Data Breach, Plaintiff Robertson was very careful about sharing her

sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Robertson would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

192. During October 2024, Plaintiff Robertson attempted to rent a car at an Avis location at Phoenix Sky Harbor International Airport. Avis refused to rent Plaintiff Robertson a vehicle because, according to its records, Plaintiff Robertson was renting a vehicle at that time from Defendants' Myrtle Beach location. In fact, the Myrtle Beach vehicle rental was charged to her corporate credit card account. However, Plaintiff Robertson was neither in Myrtle Beach, nor had she made a reservation or rented a car from the location. It was only at that point, based on conversations with Avis representatives, that she discovered that she was a victim of the Defendants' Data Breach. Plaintiff Robertson has never received a Notice directly from Defendants.

193. As a result of Avis's refusal to rent Plaintiff Robertson a car at the Phoenix Sky Harbor International Airport, Plaintiff Robertson was forced to pay for ride-share services during her time in Phoenix, and spend more money than her expected car rental costs.

194. Since then, Plaintiff Robertson spent time reviewing credit reports, reviewing various credit alerts received by text and email, checking her financial information, and dealing with increased spam text messages and emails.

195. Plaintiff Robertson suffered lost time, annoyance, interference, and inconvenience because of the Data Breach, and Plaintiff has anxiety and increased concerns for the loss of her privacy.

196. Plaintiff Robertson has suffered imminent and impending injury arising from the

present and ongoing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

197. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

198. Because of Defendants' Data Breach, Plaintiff Robertson has suffered—and will continue to suffer —from anxiety, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Robertson's injuries are precisely the type of injuries that the law contemplates and addresses.

199. Plaintiff Robertson suffered actual injury from the exposure and theft of her PII—which violates her rights to privacy.

200. Plaintiff Robertson suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

201. Plaintiff Robertson suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff Roberston's PII right in the hands of criminals.

202. Because of the Data Breach, Plaintiff Robertson anticipates spending considerable amounts of time and money to try and mitigate her injuries.

203. Today, Plaintiff Robertson has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Plaintiff Brian Harris's Experience and Injuries

204. Upon information and belief, prior to the August 2024 Data Breach, Avis

maintained Plaintiff Harris's PII in its system.

205. Plaintiff Harris provided his PII to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continue to maintain Plaintiff Harris's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

206. Plaintiff Harris reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

207. On information and belief, Plaintiff Harris's PII was accessed and stolen in the Data Breach and he has already received notice that his PII has been published by cybercriminals—or will be published imminently—on the Dark Web.

208. Plaintiff Harris has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Avis directed Plaintiff Harris to take those steps in its Notice Letter.

209. Plaintiff Harris has also spent additional time, as well as travel expenses, visiting his local Avis location in order to inquire regarding the Data Breach.

210. Further, in the aftermath of the Data Breach, Plaintiff Harris suffered from a spike in spam and scam phone calls.

211. Plaintiff Harris fears for his personal financial security and worries about what information was exposed in the Data Breach.

212. Because of Defendants' Data Breach, Plaintiff Harris has suffered—and will continue to suffer —from anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Harris's injuries are precisely the type of injuries that the law contemplates and addresses.

213. Plaintiff Harris suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

214. Plaintiff Harris suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

215. Plaintiff Harris suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff Harris's PII right in the hands of criminals.

216. Because of the Data Breach, Plaintiff Harris anticipates spending considerable amounts of time and money to try and mitigate his injuries.

217. Today, Plaintiff Harris has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

E. FTC Guidelines Prohibit Avis from Engaging in Unfair or Deceptive Acts or Practices.

218. Avis is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

219. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need

for data security should be factored into all business decision-making.[24]

220. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[25]

221. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

222. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

223. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2023, there were 3,205 publicly disclosed data compromises, affecting over 353 million victims. The U.S. specifically saw a 72% increase in data

---

[24] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[25] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

[26] *Id.*

breaches from the previous all-time high in 2021 and a 78% increase over 2022.[27] In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2019, roughly 3.5 million people reported some form of identity theft, fraud, or other consumer complaint compared to 5.4 million people in 2023.[28]

224. Rental car companies are prime targets for cybercriminals because they collect and store sensitive information including customer payment card information, personal information, government identification information, and reservation details that can be used to commit identity theft. In conjunction with this information, the rental car industry has become a new target for cybercriminals in recent years, with rental car companies Zipcar and Sixt both reporting data breaches in 2022.[29]

225. Despite being a prime target for a data breach and theft of consumer PII, Avis failed to properly implement basic data security practices. Avis's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

226. Avis was at all times fully aware of its obligations to protect its consumers' PII because of its position as a car rental company, which gave it direct access to reams of consumer PII. Avis is also aware of the significant repercussions that would result from its failure to do so.

227. Avis's failure to employ reasonable and appropriate measures to protect against

---

[27] *2023 Data Breach Report*, Identity Theft Res. Ctr. (Jan. 2024), https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.

[28] *Facts & Statistics: Identity Theft & Cybercrime*, Ins. Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Key%20Facts (last visited Sept. 30, 2024).

[29] Swagath Bandhakavi, *Car Rental Company Avis Discloses Cyberattack & Data Breach*, Tech Monitor 30 (Sept. 9, 2024), https://www.techmonitor.ai/technology/cybersecurity/car-rental-company-avis-discloses-cyberattack-and-data-breach?cf-view.

unauthorized access to confidential consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

F. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

228. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[30]

229. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

230. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to

[30] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

231. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[31]

232. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. 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, and/or use the victim's information in the event of arrest or court action.

233. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

234. Moreover, theft of PII is also gravely serious because PII is an extremely valuable

[31] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Dec. 20, 2024).

property right.[32]

235. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have resulted and will continue to result in devastating financial and personal losses to Plaintiffs.

236. As discussed above, PII is such a valuable commodity to identity thieves and, once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

237. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Avis is to get information that they can monetize by selling it on the black market for use in the kinds of criminal activity described herein. "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[33]

238. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, *they will use it.*[34] This is because there is little purpose to pursue theft

[32] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[33] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[34] *Id.*

of consumer PII unless hackers intend to profit from that information.

239. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Cybercriminals can post stolen PII on the cyber black-market for years following a data breach, thereby creating a delay before such information becomes publicly available.

240. Fraud and identity theft resulting from a data breach may therefore go undetected until debt collection calls or similar notifications of fraud commence months, or even years, later.

241. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[35]

242. Due to these risks, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[36]

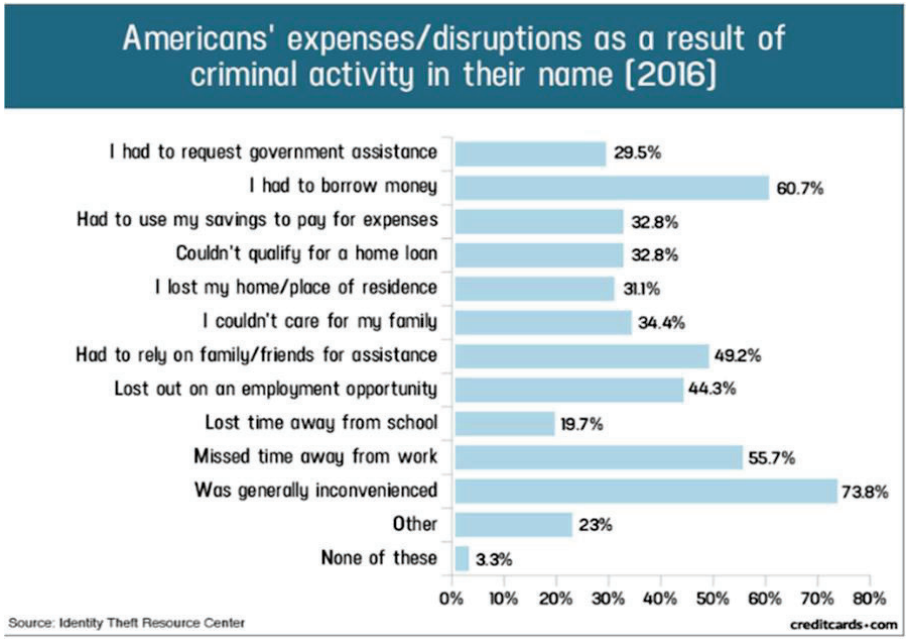
243. It is within this context that Plaintiffs must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

244. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.

---

[35] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[36] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited Dec. 20, 2024).



245. Victims of the Data Breach, like Plaintiffs, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[37]

246. As a direct and proximate result of the Data Breach, Plaintiffs had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday life, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

247. Moreover, Plaintiffs and Class members have an interest in ensuring that their PII,

[37] *Id.*

which remains in the possession of Avis, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Avis has shown itself to be wholly incapable of protecting Plaintiffs' and Class members' PII.

248. Plaintiffs and Class members also have an interest in ensuring that their personal information that was provided to Avis is removed from Avis's unencrypted files.

G. Plaintiffs Suffered Damages.

249. Avis received Plaintiffs' and Class members' PII in connection with providing car rental services. In requesting and maintaining Plaintiffs' PII for business purposes, Avis expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiffs' and Class members' PII. Avis did not, however, take proper care of Plaintiffs' and Class members' PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Avis's inadequate security measures.

250. The ramifications of Avis's failure to keep its consumers' PII secure are long-lasting and severe. Avis's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class members significant injuries and harm in several ways, including the theft of their PII as well as substantial and imminent risk of identity theft and fraud. Plaintiffs and Class members must immediately devote time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on any sensitive accounts even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in social engineering, spear phishing, or extortion attacks; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

251. In 2019, the GAO released a report addressing the steps consumers can take after a data breach.[38] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiffs and Class members) must take after a data breach, like Avis', are both time-consuming and of only limited and short-term effectiveness.

252. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[39]

253. Avis itself recognizes the certainly impending and increased risk of identity theft and fraud that Plaintiffs and Class members now face, as it has offered its current and former customers who were impacted by the Data Breach twelve months of identity protection services and further advised those individuals to "remain vigilant against incidents of identity theft and fraud" by "regularly reviewing and monitoring [their] account statements and credit history for any signs of unauthorized transactions or activity."[40]

254. Once PII is exposed, there is little that can be done to ensure that the exposed

[38] Government Accountability Off., "Data Breaches" (Mar. 2019) https://www.gao.gov/assets/gao-19-230.pdf (last visited Dec. 20, 2024).
[39] *See Identity Theft Victim Checklist*, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last visited Dec. 20, 2024).
[40] *Notice Letter*, *supra* note 4.

information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendants' conduct.

255. As a result of Defendants' 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.

256. It must also be noted there may be a substantial amount of time measured in years—between when harm occurs versus when it is discovered, and between when PII is stolen and when it is used. According to the GAO, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

257. For these reasons, Plaintiffs and Class members will need to maintain these heightened measures for years, and possibly for their entire lives, as a result of Avis's conduct.

258. Additionally, the value of Plaintiffs' and Class members' PII has been diminished by its exposure in the Data Breach. Indeed, PII is a valuable commodity to identity thieves and, once it has been compromised, criminals will use and trade the compromised PII on the cyber black market for years thereafter.[42]

259. Plaintiffs are also at a continued risk because their information remains in Avis's computer systems, which have already been shown to be susceptible to compromise and attack,

[41] *See* 2007 GAO Report, at 29.
[42] *The Price Cybercriminals Charge for Stolen Data*, Trustwave (Aug. 6, 2023), https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-price-cybercriminals-charge-for-stolen-data/ (last visited Sept. 30, 2024).

and their PII is subject to further attack so long as Avis fails to undertake the necessary and appropriate security and training measures to protect its customers' PII.

260. In addition, Plaintiffs and Class members have suffered emotional distress because of the Data Breach, and the increased risk of identity theft and financial fraud.

CLASS ALLEGATIONS

261. Plaintiffs bring all counts, as set forth below, individually and as a class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Nationwide Class, as well as the following State Subclasses (also collectively referred to herein as the "Class" or "Classes"), subject to amendment as appropriate:

Nationwide Class:

> All individuals residing in the United States whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter.
> (the "Nationwide Class").

California Subclass:

> All individuals residing in California whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter (the "California Subclass").

Illinois Subclass:

> All residents of Illinois whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter (the "Illinois Subclass").

Florida Subclass:

> All residents of Florida whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter (the "Florida Subclass").

Texas Subclass:

> All residents of Texas whose Private Information was accessed and/or acquired as

a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter (the "Texas Subclass").

Minnesota Subclass:

All residents of Minnesota whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter (the "Minnesota Subclass").

South Carolina Subclass:

All residents of South Carolina whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter (the "South Carolina Subclass").

Alabama Subclass:

All residents of Alabama whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter (the "Alabama Subclass").

Oklahoma Subclass:

All residents of Oklahoma whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter (the "Oklahoma Subclass").

Tennessee Subclass:

All residents of Tennessee whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter (the "Tennessee Subclass").

Kansas Subclass:

All residents of Kansas whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about September 4, 2024 or thereafter (the "Kansas Subclass").

262. Excluded from the Class(es) are Defendants, their subsidiaries and affiliates, officers and directors, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to

whom this action is assigned, and the members of their immediate families.

263. This proposed Class definitions are based on the information available to Plaintiffs currently. Plaintiffs may modify the Class definitions in an amended pleading or when they move for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

264. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiffs are informed and believe, and thereon allege, that there are, at a minimum, approximately 300,000 members of the Classes described above. The exact size of the Classes and the identities of the individual members are identifiable through Avis's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Classes include approximately 300,000 individuals.

265. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Classes. Such common questions include, but are not limited to:

a. Whether Avis had a duty to protect Plaintiffs' and Class members' PII;

b. Whether Avis was negligent in collecting and storing Plaintiffs' and Class members' PII, and breached its duties thereby;

c. Whether Avis breached its fiduciary duty to Plaintiffs and the Classes;

d. Whether Avis breached its duty of confidence to Plaintiffs and the Classes;

e. Whether Avis violated its own Privacy Policy;

f. Whether Avis entered a contract with Plaintiffs and the Classes;

g. Whether an implied contract existed between Class members and Defendants providing that Defendants would implement and maintain reasonable security measures to protect and secure Plaintiffs' and Class members' PII from unauthorized access and disclosure;

h. Whether Avis breached that contract by failing to adequately safeguard Plaintiffs' and Class members' PII;

i. Whether Avis was unjustly enriched;

j. Whether Plaintiffs and Class members are entitled to damages because of Avis's wrongful conduct; and

k. Whether Plaintiffs and Class members are entitled to restitution because of Avis's wrongful conduct.

266. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs' claims are typical of the claims of the members of the Classes. The claims of the Plaintiffs and members of the Classes are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Classes all had information stored in Avis's System, each having their PII exposed and/or accessed by an unauthorized third party.

267. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs are adequate representatives of the Classes because their interests do not conflict with the interests of the other Class members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel have adequate financial means to vigorously pursue this action and ensure the interests of the Classes will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

268. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendants have acted and/or refused to act on grounds that apply generally to the Classes therefore making injunctive and/or declarative relief appropriate with respect to the Classes under Rule 23(b)(2).

269. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is superior to other available

methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Avis. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

270. Avis has acted on grounds that apply generally to the Classes as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

271. Likewise, particular issues are appropriate for certification because these claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Avis failed to timely and adequately notify the public of the Data Breach;

b. Whether Avis owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Avis's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Avis's failure to institute adequate protective security measures amounted to negligence;

e. Whether Avis failed to take commercially reasonable steps to safeguard consumer

PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

272. Finally, all members of the proposed Classes are readily ascertainable. Avis has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

COUNT I
NEGLIGENCE
(By Plaintiffs on behalf of the Classes)

273. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

274. Plaintiffs bring this claim individually and on behalf of the Class**es**.

275. Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their PII in their possession, custody, and control.

276. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

277. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

278. Defendants' duty also arose from Defendants' position as a car rental agency that collects its customers' PII. Defendants thereby assumed a duty to reasonably protect consumers'

information.

279. Defendants breached the duties they owed to Plaintiffs and Class members and thus were negligent. As a result of a successful attack directed towards Defendants that compromised Plaintiffs' and Class members' PII, Defendants breached their duties through some combination of the following errors and omissions that allowed the data compromise to occur:

(a) mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies and practices published to their customers; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

280. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class members, their PII would not have been compromised.

281. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and

unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who

likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

282. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*
(By Plaintiffs on behalf of the Classes)

283. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

284. Plaintiffs bring this claim individually and on behalf of the Classes.

285. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

286. Avis violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of a data breach involving PII of their customers.

287. Plaintiffs and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

288. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

289. The harm that has occurred because of Defendants' conduct is the type of harm that

the FTC Act and Part 2 were intended to guard against.

290. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
BREACH OF CONTRACT
(By Plaintiffs on behalf of the Classes)

291. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

292. Plaintiffs bring this claim individually and on behalf of the Classes.

293. Plaintiffs and Class members entered into a valid and enforceable contract through which they paid money to Avis in exchange for services. That contract included promises by Defendants to secure, safeguard, and not disclose Plaintiffs' and Class members' Private Information.

294. Avis's Privacy Policy memorialized the rights and obligations of Avis and its customers. This document was provided to Plaintiffs and Class members in a way in which it became part of the agreement for services.

295. In its Privacy Policy, Avis commits to protecting the privacy and security of its customers' private information.

296. Plaintiffs and Class members fully performed their obligations under their contracts with Avis.

297. However, Avis did not secure, safeguard, and/or keep private Plaintiffs' and Class members' Private Information, and therefore Avis breached its contracts with Plaintiffs and Class members.

298. Avis allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class members' Private Information without permission. Therefore, Avis breached the Privacy Policy with Plaintiffs and Class members.

299. Avis's failure to satisfy its confidentiality and privacy obligations resulted in Avis providing services to Plaintiffs and Class members that were of diminished value.

300. As a result, Plaintiffs and Class members have been harmed, damaged, and/or injured as described herein, including in Avis's failure to fully perform its part of the bargain with Plaintiffs and Class members.

301. As a direct and proximate result of Avis's conduct, Plaintiffs and Class members suffered and will continue to suffer damages in an amount to be proven at trial.

302. In addition to monetary relief, Plaintiffs and Class members are also entitled to injunctive relief requiring Avis to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(By Plaintiffs on behalf of the Classes)

303. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

304. Plaintiffs bring this claim individually and on behalf of the Classes.

305. When Plaintiffs and Class members provided their PII to Defendants in exchange for car rental services, they entered into implied contracts with Defendants, under which Defendants agreed to take reasonable steps to protect Plaintiffs' and Class members' PII, comply with statutory and common law duties to protect their PII, and timely notify them in the event of

a data breach.

306. Defendants solicited and invited Plaintiffs and Class members to provide their PII as part of Defendants' provision of services. Plaintiffs and Class members accepted Defendants' offers and provided their PII to Defendants.

307. When entering into implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendants' data security practices complied with their statutory and common law duties to adequately protect Plaintiffs' and Class members' PII and to timely notify them in the event of a data breach.

308. Defendants' implied promise to safeguard consumers' PII is evidenced by, *e.g.*, the representations in Defendants' Notice of Privacy Practices set forth above.

309. Plaintiffs and Class members paid money to Defendants to receive services. Plaintiffs and Class members reasonably believed and expected that Defendants would use part of those funds to obtain and provide adequate data security. Defendants failed to do so.

310. Plaintiffs and Class members would not have provided their PII to Defendants had they known that Defendants would not safeguard their PII, as promised, or provide timely notice of a data breach.

311. Plaintiffs and Class members fully performed their obligations under their implied contracts with Defendants.

312. Defendants breached their implied contracts with Plaintiffs and Class members by failing to safeguard Plaintiffs' and Class members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

313. The losses and damages Plaintiffs and Class members sustained include, but are not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class

members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

314. As a direct and proximate result of Defendants' breach of contract, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT V
BREACH OF FIDUCIARY DUTY
(By Plaintiffs on behalf of the Classes)

315. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

316. Plaintiffs bring this claim individually and on behalf of the Classes.

317. Plaintiffs and Class members have an interest, both equitable and legal, in their PII that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

318. As a recipient of consumers' PII, Defendants have a fiduciary relationship to Plaintiffs and the Class members.

319. Because of that fiduciary relationship, Defendants were provided with and stored private and valuable PII related to Plaintiffs and Class members. Plaintiffs and Class members were entitled to expect their information would remain confidential while in Defendants' possession.

320. Defendants owed a fiduciary duty under common law to Plaintiffs and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and

protecting their PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

321. As a result of the parties' fiduciary relationship, Defendants had an obligation to maintain the confidentiality of the PII within Plaintiffs' and the Class members' personal records.

322. Plaintiffs and Class members have a privacy interest in personal matters, and Avis had a fiduciary duty not to disclose their data.

323. Defendants had possession and knowledge of confidential PII of Plaintiffs and Class members, information not generally publicly known.

324. Plaintiffs and Class members did not consent to nor authorize Defendants to release or disclose their PII to unknown criminal actors.

325. Defendants breached their fiduciary duties owed to Plaintiffs and Class members by, among other things:

a. mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

b. mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust their information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time

thereafter;

g. failing to follow their own privacy policies and practices published to their customers; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

326. But for Defendants' wrongful breach of their fiduciary duties owed to Plaintiffs and Class members, their PII would not have been compromised.

327. As a direct and proximate result of Defendants' breach, Plaintiffs and Class members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased

risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

328. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT VI
BREACH OF CONFIDENCE
(By Plaintiffs on behalf of the Classes)

329. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

330. Plaintiffs bring this claim individually and on behalf of the Classes.

331. Plaintiffs and Class Member have an interest, both equitable and legal, in their PII

that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

332. As a service provider collecting PII, Defendants have a special relationship to their customers, like Plaintiffs and the Class members.

333. Plaintiffs and Class members provided Defendants with their personal and confidential PII under both the express and/or implied agreement of Defendants to limit the use and disclosure of such PII.

334. Defendants owed a duty to Plaintiffs and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in their possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

335. As a result of the parties' relationship, Defendants had possession and knowledge of confidential PII of Plaintiffs and Class members.

336. Plaintiffs' and Class members' PII is not generally known to the public and is confidential by nature.

337. Plaintiffs and Class members did not consent to nor authorize Defendants to release or disclose their PII to unknown criminal actors.

338. Defendants breached the duties of confidence they owed to Plaintiffs and Class members when their PII was disclosed to unknown criminal hackers.

339. Defendants breached their duties of confidence by failing to safeguard Plaintiffs' and Class members' PII, including by, among other things: (a) mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of

PII; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies and practices published to their customers; (h) storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class members' PII to criminal third parties.

340. But for Defendants' wrongful breach of their duty of confidence owed to Plaintiffs and Class members, their privacy, confidence, and PII would not have been compromised.

341. As a direct and proximate result of Defendants' breach of Plaintiffs' and Class members' confidence, Plaintiffs and Class members have suffered injuries, including:

a. The erosion of the essential and confidential relationship between Defendants – as a car rental agency – and Plaintiffs and Class members as parties that were subject to the car rental agreement;

b. Theft of their PII;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data.

342. Additionally, Defendants received payments from entities on behalf of Plaintiffs and Class members for services with the understanding that Defendants would uphold their responsibilities to maintain the confidence of Plaintiffs' and Class members' private information.

343. Defendants breached the confidence of Plaintiffs and Class members when it made an unauthorized release and disclosure of their confidential information and, accordingly, it would be inequitable for Defendants to retain the benefit at Plaintiffs' and Class members' expense.

344. As a direct and proximate result of Defendants' breach of its duty of confidence, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VII
INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(By Plaintiffs on behalf of the Classes)

345. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

346. Plaintiffs bring this claim individually and on behalf of the Classes.

347. Plaintiffs and Class members had a reasonable expectation of privacy in the PII Defendants mishandled.

348. Defendants' conduct as alleged above intruded upon Plaintiffs' and Class members' seclusion under common law.

349. By intentionally failing to keep Plaintiffs' and Class members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiffs' and Class members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class members' private affairs in a manner that identifies Plaintiffs and Class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class members.

350. Defendants knew that an ordinary person in Plaintiffs' or Class members' position would consider Defendants' intentional actions highly offensive and objectionable.

351. Defendants invaded Plaintiffs' and Class members' right to privacy and intruded into Plaintiffs' and Class members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

352. Defendants intentionally concealed from and delayed reporting to Plaintiffs and Class members a security incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

353. The conduct described above was directed at Plaintiffs and the Class members.

354. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendants' conduct amounted to a substantial and serious invasion of Plaintiffs' and Class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

355. In failing to protect Plaintiffs' and Class members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Class members.

356. As a direct and proximate result of Avis's conduct, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT VIII
UNJUST ENRICHMENT
(By Plaintiffs on behalf of the Classes)

357. Plaintiffs restate and reallege the preceding allegations above as if fully alleged

herein.

358. Plaintiffs bring this claim individually and on behalf of the Classes.

359. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including payments made by or on behalf of Plaintiffs and the Class members.

360. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

361. Plaintiffs and Class members conferred a monetary benefit on Defendants. In exchange, Plaintiffs and Class members should have received from Defendants the goods and services that were the subject of the transaction and had their PII protected with adequate data security.

362. Defendants knew that Plaintiffs and Class members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the PII of Plaintiffs and Class members for business purposes.

363. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security.

364. Under the principles of equity and good conscience, Defendants should not be

permitted to retain the money belonging to Plaintiffs and Class members, because Defendants failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

365. Defendants failed to secure Plaintiffs' and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class members provided.

366. Defendants acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

367. If Plaintiffs and Class members knew that Defendants had not reasonably secured their PII, they would not have agreed to have their information provided to Defendants.

368. Plaintiffs and Class members have no adequate remedy at law.

369. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection

services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

370. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

371. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class members overpaid for Defendants' services.

COUNT IX
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT,

CAL. CIV. CODE § 1798.100, *et seq.*
(On behalf of Plaintiffs Lopez and Harris and the California Subclass)

372. Plaintiffs Lopez and Harris (for purposes of this count, "Plaintiffs") restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

373. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiffs' and California Subclass members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure because of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiffs and California Subclass members.

374. As a direct and proximate result of Defendants' acts, Plaintiffs' and the California Subclass members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendants' computer systems and/or from the dark web, where hackers further disclosed Defendants' customers' PII.

375. As a direct and proximate result of Defendants' acts, Plaintiffs and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of California Subclass members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

376. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard California Subclass members' PII and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiffs and the California Subclass members.

377. Defendant Avis Rent A Car System, LLC, is a subsidiary of Avis Budget Group, Inc. Avis employs more than 24,500 people and generates approximately $12 billion in annual revenue. It collects consumers' PII as defined in California Civil Code § 1798.140.

378. Plaintiffs Lopez and Harris and California Subclass members are "consumer[s]" as defined by Cal. Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

379. Defendants are "businesses" as that term is defined in Cal. Civ. Code § 1798.140(d). Defendants are organized or operated for the profit or financial benefit of their shareholders or owners. Defendants collect consumers' personal information (including that of Plaintiffs Lopez and Harris and the California Subclass) or such information is collected on Defendants' behalf, and Defendants determine the purposes and means of processing of consumers' personal information. Defendants do business in California and have annual revenues well in excess of $25 million dollars.

380. The information accessed during the Data Breach constitutes "personal information" as that term is defined in Cal. Civ. Code § 1798.140(v)(1). At minimum, that information included full names, mailing addresses, driver's license numbers.

381. Under the CCPA, Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information that it stored. Cal. Civ. Code § 798.150(1)

382. Defendants' failure to prevent the Data Breach by implementing and maintaining reasonable security procedures and practices constitutes a breach of their duties under the CCPA.

383. On November 4, 2024, Plaintiff Lopez provided written notice to Defendants

identifying the specific provisions of this Act he alleges they have violated.[43] On November 20, 2024, Defendants denied all allegations.

384. On September 20, 2024, Plaintiff Harris provided written notice to Defendants identifying the specific provisions of this Act he alleges they have violated. Defendants did not respond to Plaintiff Harris's notice, and therefore are deemed to have not cured the Data Breach within 30 days of the notice. Plaintiff Harris seeks the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty dollars ($750) per consumer per incident or actual damages, whichever is greater, together with injunctive relief. *See* CAL. CIV. CODE § 1798.150(b).

COUNT X
Violations of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201, et seq.
(On behalf of Plaintiff Pestano and the Florida Subclass)

385. Plaintiff Pestano (for purposes of this count, "Plaintiff") restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

386. Fla. Stat. § 501.201, et seq. is expressly intended to protect consumers like Plaintiff and Florida Subclass members from unfair or deceptive trade practices. Plaintiff and Florida Subclass members have a vested interest in the privacy, security and integrity of their Private Information, and therefore, this interest is a "thing of value" as contemplated by FDUTPA.

387. Avis is a "person" within the meaning of FDUTPA and, at all pertinent times, was subject to FUDPTA's requirements and proscriptions with respect to all of Avis's business and trade practices described herein.

388. Avis engaged in unfair and deceptive trade practices by creating a false expectation

[43] See CCPA Notice of Claim, attached as Exhibit B.

of privacy to Florida consumers, including Plaintiff and Florida Subclass members, through representations and promises that their Private Information in Avis's custody will be kept safe through adequate and reasonable data security measures that comply with the FTC Act and industry standards, while in reality Avis failed to take commercially reasonable steps to protect the Private Information entrusted to it.

389. Avis engaged in deceptive and unfair acts and practices, misrepresentations, and the concealment and omission of material facts in connection with the sale and advertisement of services in violation of FDUTPA, including without limitation by the following:

a. Failing to maintain adequate data security to keep Plaintiff's and Florida Subclass members' sensitive Private Information from being accessed and taken by cybercriminals;

b. Failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTCA;

c. Failing to disclose and omitting materials facts to Plaintiff and Florida Subclass members regarding Avis's lack of adequate data security and inability or unwillingness to properly secure and protect Plaintiff's and Florida Subclass members' Private Information;

d. Failing to disclose and/or omitting materials facts to Plaintiff and Florida Subclass members about Avis's failure to comply with relevant federal and state laws on the privacy and security of Plaintiff's and Florida Subclass members' Private Information; and

e. Failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Florida Subclass members'

Private Information from further unauthorized disclosure, release, breaches, and theft.

390. These actions also constitute deceptive and unfair acts or practices because Avis knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and Florida Subclass members, and would erase the false impression of adequate security for their Private Information if known.

391. But for Avis's unfair acts and practices and deceptive misrepresentations and omissions, Plaintiff and Florida Subclass members would have known the truth about Avis's inadequate data security measures and would not have provided their Private Information to, or entered into transactions with, Avis.

392. Avis's wrongful practices were and are injurious to the public because they were and are part of its generalized course of conduct that applied to the Florida Subclass as a whole. Plaintiff, Florida Subclass members, and the public have been adversely affected by Avis's conduct and the public was and is at risk as a result thereof.

393. Plaintiff and Florida Subclass members are consumers "likely to be damaged" by Avis's ongoing deceptive trade practices.

394. Avis's unfair conduct as described herein was directed and emanated from its Florida business operations to the detriment of Plaintiff and Florida Subclass members in Florida.

395. Plaintiff and Florida Subclass members have standing to pursue this claim because, as a direct and proximate result of Avis's violations of FDUTPA, Plaintiff and Florida Subclass members have been "aggrieved" by a violation of FDUTPA and bring this action to obtain a declaratory judgment that Avis's acts or practices violate FDUTPA. *See* Fla. Stat. § 501.211(a).

396. Plaintiff and Florida Subclass members also have standing to pursue this claim because, as a direct result of Avis's knowing violations of FDUTPA, Plaintiff and Florida Subclass members are at a substantial present and imminent risk of identity theft. Avis still possesses Plaintiff's and Florida Subclass members' Private Information, which has already been accessed by unauthorized third parties, evidencing a substantial and imminent risk of future identity theft for Plaintiff and the Florida Subclass.

397. Plaintiff and Florida Subclass members are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, including, but not limited to:

a. ordering that Avis engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Avis's systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

b. ordering that Avis engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Avis audit, test, and train security personnel regarding any new or modified procedures;

d. ordering that Avis segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering that Avis purge, delete, and destroy Private Information not necessary for its provisions of services in a reasonably secure manner;

f. ordering that Avis conduct regular database scans and security checks;

g. ordering that Avis routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Avis to meaningfully educate individuals about the threats they face because of the loss of their financial and Private Information to third parties, as well as the steps victims should take to protect themselves.

398. Plaintiff brings this action individually and on behalf of the Florida Subclass for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, the Florida Subclass, and the public from Avis's unfair methods of competition and unfair, unconscionable, and unlawful practices. Avis's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

399. The above unfair, unconscionable, and unlawful practices and acts by Avis were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Florida Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

400. Avis's actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

401. Plaintiff and Florida Subclass members seek relief under FDUTPA, Fla. Stat. §§ 501.201, et seq., including, but not limited to, a declaratory judgment that Avis's actions and/or practices violate FDUTPA.

402. Under FDUTPA, Plaintiff and Florida Subclass members are entitled to preliminary

and permanent injunctive relief without proof of monetary damage, loss of profits, or intent to deceive. Plaintiff and Florida Subclass members seek equitable relief and to enjoin Avis on terms that the Court considers appropriate.

403. Avis's conduct in violation of FDUTPA caused and continues to cause substantial injury to Plaintiff and Florida Subclass members. Unless preliminary and permanent injunctive relief is granted, Plaintiff and Florida Subclass members will suffer harm. Plaintiff and Florida Subclass members do not have an adequate remedy at law, and the balance of the equities weighs in favor of Plaintiff and Florida Subclass members, the victims of Avis's unfair and deceptive conduct.

404. At all material times, Avis's unfair and deceptive trade practices were willful within the meaning of FDUTPA and, accordingly, Plaintiff and Florida Subclass members are entitled to an award of attorneys' fees, costs and other recoverable expenses of litigation.

COUNT XI
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, et seq.
(On behalf of Plaintiff Tatiyaratana and the Illinois Subclass)

405. Plaintiff Tatiyaratana (for purposes of this Count, "Plaintiff") restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

406. Plaintiff and the Illinois Subclass are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Illinois Subclass, and Defendants are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

407. Defendants engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendants engage in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

408. Defendants engaged in deceptive and unfair acts and practices, misrepresentation,

and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiff's and the Illinois Subclass members' sensitive Private Information from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting materials facts to Plaintiff and the Illinois Subclass regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the Private Information of Plaintiff and the Illinois Subclass; (iii) failing to disclose or omitting material facts to Plaintiff and the Illinois Subclass about Defendants' failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Private Information of Plaintiff and the Illinois Subclass; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Illinois Subclass's Private Information and other PII from further unauthorized disclosure, release, data breaches, and theft.

409. These actions also constitute deceptive and unfair acts or practices because Defendants knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Illinois Subclass and defeat their reasonable expectations about the security of their Private Information.

410. Defendants intended that Plaintiff and the Illinois Subclass rely on their deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendants' offering of services.

411. Defendants' wrongful practices were and are injurious to the public because those practices were part of Defendants' generalized course of conduct that applied to the Illinois

Subclass. Plaintiff and the Illinois Subclass have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

412. As a result of Defendants' wrongful conduct, Plaintiff and the Illinois Subclass were injured in that they never would have provided their Private Information to Defendants, or purchased Defendants' services, had they known or been told that Defendants failed to maintain sufficient security to keep their Private Information from being hacked and taken and misused by others.

413. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff and the Illinois Subclass have suffered harm, including: (i) the loss of the opportunity how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Illinois Subclass Members.

414. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a

result of Defendants' violations of the CFA.

COUNT XII
Violation of the New Jersey Consumer Fraud Act N.J.S. § 56:8-1, et seq.
(By Plaintiffs on behalf of the Nationwide Class)

415. Plaintiffs and Nationwide Class members restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

416. The New Jersey Consumer Fraud Act ("NJCFA") protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

417. The NJCFA prohibits any unlawful, unfair, or fraudulent business acts or practices including the employment of any deception, fraud, false pretense, false promise, false advertising, misrepresentation, or the concealment, suppression, or omission of any material fact.

418. The NJCFA applies to Defendants' actions and conduct as described herein because it protects consumers in transactions that are intended to result, or which have resulted, in the sale of goods or services.

419. Defendants are a "person" as defined under section 56:8-1(d) of the NJCFA.

420. Defendants' conduct as alleged herein relates to "sale" as defined by section 56:8-1(e) of the NJCFA.

421. Plaintiffs and the members of the Nationwide Class are each a "person" as defined under section 56:8-1(d) of the NJCFA.

422. Defendants advertise, offer, and sell "merchandise" as defined by section 56:8-1(d) of the NJCFA.

423. Defendants advertise, offer, or sell goods or services in New Jersey and elsewhere and engage in trade or commerce directly or indirectly affecting the people of New Jersey.

424. Defendants engaged in unfair and deceptive practices in violation of the NJCFA,

by:

a. Making false or misleading oral and written representations with the capacity or tendency, or effect, of deceiving or misleading consumers;

b. Failing to state a material fact where the failure deceives or intends to deceive;

c. Advertising or offering consumer goods or services without intent to sell them as advertised or offered; and

d. Engaging in deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement.

425. Defendants engaged in these unfair and deceptive trade practices in connection with the sale or selling of consumer goods or services, in violation of the NJCFA, by:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the Nationwide Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Nationwide Class members' PII, including duties imposed by the Section 5 of the FTC Act, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect Plaintiffs' and the Nationwide Class members' PII;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Nationwide Class members' PII, including duties by Section 5 of the FTC Act, which was a direct and proximate cause of the Data Breach; and.

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and the Nationwide Class members' PII.

426. Defendants were aware or should have been aware that they were not implementing security protections as outlined above.

427. Defendants acted intentionally, knowingly, and maliciously to violate the NJCFA, as they were on notice of the possibility of the Data Breach due to the massive proliferation of cybersecurity incidents in recent years.

428. Defendants intended to mislead Plaintiffs and the Nationwide Class members and induce them to rely on their misrepresentations and omissions.

429. Defendants' misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' personal and confidential information.

430. Had Defendants not engaged in the deceptive omission of material facts described above, Plaintiffs and the Nationwide Class members would have been presented with an informed choice as to whether or not to purchase products and services from Defendants.

431. Plaintiffs and the Nationwide Class members were injured by Defendants' unfair and deceptive acts, and will continue to suffer injury, ascertainable losses of money or property,

and monetary and nonmonetary damages. This includes damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased imminent risk of fraud and identity theft, and the loss of value of their PII.

432. Had Defendants disclosed their true security practices, Plaintiffs and the Nationwide Class members either would not have purchased products or services from the Defendants or would have paid substantially less for them.

433. As a direct and proximate result of Defendants' violation of the NJCFA, Plaintiffs and each member of the Nationwide Class have suffered harm in the form of monies paid for Defendants' products and/or services.

434. Plaintiffs, on behalf of themselves and the Nationwide Class members, seek an order (1) requiring Defendants to cease the unfair practices described herein; (2) awarding damages, including treble damages, interest, and reasonable attorneys' fees, expenses, and costs to the extent allowable; and/or (3) requiring Defendants to restore to Plaintiffs and members of the Nationwide Class any money acquired by means of unfair competition (restitution).

COUNT XIII
DECLARATORY JUDGMENT
(By Plaintiffs on behalf of the Classes)

435. Plaintiffs restate and reallege the preceding allegations the paragraphs above as if fully alleged herein.

436. Plaintiffs bring this claim individually and on behalf of the Classes.

437. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

438. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' PII, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their PII. Plaintiffs and the Class members remain at imminent risk that additional compromises of their PII will occur in the future.

439. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

440. Defendants still possess Plaintiffs' and Class members' PII.

441. Defendants have made no announcement that they have changed their data storage or security practices relating to the storage of Plaintiffs' and Class members' PII.

442. To Plaintiffs' knowledge, Defendants have made no announcement or notification that they have remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

443. If an injunction is not issued, Plaintiffs and the Class members will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Avis. The risk of another such breach is real, immediate, and substantial.

444. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs at Avis, Plaintiffs and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing

reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

445. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Avis, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other consumers whose PII would be further compromised.

446. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Avis implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Avis's systems on a periodic basis, and ordering Avis to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and

what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

a. For an Order certifying this action as a class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b. For equitable relief enjoining Avis from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

c. For equitable relief compelling Avis to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Avis's wrongful conduct;

e. Ordering Avis to pay for not less than three years of credit monitoring services for Plaintiffs and the Class members;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded by Plaintiffs on all claims so triable.

Dated: December 20, 2024

Respectfully submitted,

By: /s/ *David DiSabato*
David J. DiSabato, Esq.
Tyler J. Bean, Esq.
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com

Plaintiffs' Liaison Counsel

Liberato P. Verderame (ID# 032251997)
Marc H. Edelson*
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
Tel: (215) 867-2399
E: lverderame@edelson-law.com
E: medelson@edelson-law.com

Gregory Haroutunian (ID No. 051212013)
Anderson Berry
CLAYEO C. ARNOLD, A PROFESSIONAL CORP
865 Howe Avenue
Sacramento, CA 95825
Tel: (916) 777-7777
Fax: (916) 924-1829
E: gharoutunian@justice4you.com

Gary F. Lynch
Connor Hayes*
LYNCH CARPENTER LLP
1133 Penn Avenue
5th Floor
Pittsburgh, PA 15222

Tel: 412.253.6307
Office: 412.322.9243
Fax: 412.231.0246
E: gary@lcllp.com
E: connorh@lcllph.com

Plaintiffs' Interim Co-Lead Counsel

James C. Shah
Alec J. Berin
MILLER SHAH LLP
1845 Walnut Street, Suite 806
Philadelphia, PA 19103
Tel: (866) 540-5505
Fax: (866) 300-7367
E: jcshah@millershah.com
E ajberin@millershah.com

James E. Cecchi
CARELLA BYRNE CECCHI BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
Tel : (973) 994-1700
Fax: (973) 994-1744
E: jcecchi@carellabyrne.com

Amber L. Schubert*
Daniel L.M. Pulgram*
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: (415)788-4220
Fax: (415) 788-0161
E: aschubert@sjk.law
E: dpulgram@sjk.law

Kevin Laukaitis, Esq.
LAUKAITIS LAW LLC
(N.J. Id: #155742022)
954 Avenida Ponce De León
Suite 205, #10518
San Juan, Puerto Rico 00907
E: klaukaitis@laukaitislaw.com

Kent A. Bronson, Esq.*
BRONSON LEGAL LLC
1216 Broadway, 2nd Floor
New York, NY 10001
Tel: (212) 594-5300
Fax: (212) 868-1229
E: kbronson@bronsonlegalllc.com

Janine L. Pollack (NJ Bar No. 041671989)
GEORGE FELDMAN MCDONALD, PLLC
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel: (917) 983-2707
Fax: (888) 421-4173
E: jpollack@4-justice.com
E-Service: eService@4-justice.com

Lori G. Feldman, Esq.*
GEORGE FELDMAN MCDONALD, PLLC
102 Half Moon Bay Drive Croton-on-Hudson, NY 10520
Tel: (917) 983-9321
Fax: (888) 421-4173
E: lfeldman@4-justice.com
E-Service: eService@4-justice.com

Patrick Yarborough*
FOSTER YARBOROUGH PLLC
917 Franklin Street, Suite 220
Houston, TX 77002
Tel: (713) 331-5254
Fax: (713) 513-5202
E: patrick@fosteryarborough.com
E-Service: patrick@ecf.courtdrive.com

Patrick Howard (NJ Atty ID #02280-2001)
SALTZ MONGELUZZI & BENDESKY, P.C.
8000 Sagemore Drive, Suite 8303
Marlton, NJ 08053
Tel: (856) 751-0868

E: phoward@smbb.com

Joe P. Leniski, Jr.*
HERZFELD, SUETHOLZ, GASTEL, LENISKI and WALL, PLLC
223 Rosa L. Parks Avenue, Suite 300
Nashville, Tennessee 37203
Tel: (615) 800-6225
E: joey@hsglawgroup.com

Peter J. Jannace*
HERZFELD, SUETHOLZ, GASTEL, LENISKI and WALL, PLLC
515 Park Avenue
Louisville, Kentucky 40208
Tel: (502) 636-4333
E: peter@hsglawgroup.com

Mark C. Rifkin*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
270 Madison Avenue
New York, New York 10016
Tel: 212/545-4600
Fax: 212/545-4677
E: rifkin@whafh.com

Rachele R. Byrd*
Stephanie Aviles*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, California
Tel: (619) 239-4599
Fax: (619) 234-4599
E: byrd@whafh.com
E: saviles@whafh.com

Jon Tostrud*
Anthony Carter*
TOSTRUD LAW GROUP, PC
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Tel: (310) 278-2600
Fax: (310) 278-2640

E: jtostrud@tostrudlaw.com
E: acarter@tostrudlaw.com

Attorneys for Plaintiffs and the Putative Class
* *Pro Hac Vice* anticipated