UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

BROOKE PESTANO and JENNIFER SIGNORILE, on behalf of themselves and all others similarly situated, Plaintiffs, v. **AVIS RENT A CAR SYSTEM, LLC**, and **AVIS BUDGET GROUP, INC.** Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Brooke Pestano and Jennifer Signorile ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Avis Rent A Car System, LLC and Avis Budget Group, Inc. (collectively, "Avis" or "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Avis for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Avis customers' name, driver's license number, date of birth, credit card number and expiration date, and phone number (the "Private Information") from hackers.

2. Avis, headquartered in Parsippany, New Jersey, is a rental car service company that serves hundreds of thousands of customers nationwide.

3. On or about September 5, 2024, Avis filed official notice of a hacking incident with the Office of the Maine Attorney General.

4. On or about September 4, 2024, Avis also sent out data breach letters to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice filed by the company, on August 5, 2024, Avis discovered that "an unauthorized third party gained access to one of our business applications."[1] detected unusual activity on some of its computer systems. In response, the company launched an investigation. The Avis investigation revealed that an unauthorized party had access to certain company files between August 3, 2024, and August 6, 2024 (the "Data Breach").

6. Plaintiffs and "Class Members" (defined below) 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.

7. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, credit card numbers and expiration dates, driver's license number, and date of birth that Avis collected and maintained.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by Avis that all personal data or copies of data have been recovered or destroyed, or that Defendants have adequately enhanced their data security practices sufficient to avoid a similar breach of its network in the future.

[1] *See* Notice Letter https://www.maine.gov/cgi-bin/agviewerad/ret?loc=1225 (last visited Sept. 17, 2024).

10. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiffs bring this class action lawsuit to address Avis's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

12. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Avis, and thus Avis was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, Avis and its employees failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had Avis properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiffs' and Class Members' identities are now at risk because of Avis's negligent conduct as the Private Information that Avis collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence per se, breach of contract, breach of implied contract, unjust enrichment, declaratory judgment, and violations of Illinois and Florida consumer protection statutes.

II. PARTIES

17. Plaintiff Brooke Pestano is, and at all times mentioned herein was, an individual citizen of the State of Florida.

18. Plaintiff Jennifer Signorile is, and at all times mentioned herein was, an individual citizen of the State of Illinois.

19. Defendant Avis Rent A Car System, LLC is a rental car service company with its principal place of business at 379 Interpace Parkway, Parsippany, New Jersey, 07054. Avis Rent A Car System, LLC, is an affiliate subsidiary of Avis Budget Group, Inc.

20. Defendant Avis Budget Group, Inc. is the parent company of Avis Rent A Car System, LLC, with its principal place of business at 379 Interpace Parkway, Parsippany, New Jersey, 07054.

III. JURISDICTION AND VENUE

21. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Avis. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

22. This Court has jurisdiction over Avis because Avis operates in and/or is incorporated in this District.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Avis has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Avis's Business and Collection of Plaintiffs' and Class Members' Private Information

24. Avis is a rental car service company. Founded in 1946, Avis is a premier car rental service company with approximately 5,500 locations in more than 165 countries, serving hundreds of thousands of customers in the United States. 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.[2]

25. As a condition of receiving rental car services, Avis requires that its customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from Avis, Plaintiffs and Class Members were required to provide their Private Information to Defendants.

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

27. In its notice letter, Avis states that "[w]e take the privacy and security of our customers' information seriously."[3] In its privacy policy, Avis informs its customers that "[w]e take reasonable steps designed to protect personal information from unauthorized use, access, disclosure, alteration, destruction or loss."[4] 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

[2] *See* https://www.avisbudgetgroup.com/about-us/ (last visited Sept. 17, 2024).
[3] *See* Notice Letter.
[4] See https://www.avis.com/en/legal-documents/privacy-notice (last visited Sept. 17, 2024).

> 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.[5]

28. Because of the highly sensitive and personal nature of the information Avis acquires and stores with respect to its customers, Avis, upon information and belief, promises to, among other things: keep customers' Private Information private; comply with industry standards related to data security and the maintenance of its customers' Private Information; inform its customers of its legal duties relating to data security and comply with all federal and state laws protecting customers' Private Information; only use and release customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers if their Private Information is disclosed without authorization.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Avis assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

30. Plaintiffs and Class Members relied on Avis to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendants ultimately failed to do.

B. <u>The Data Breach and Avis's Inadequate Notice to Plaintiffs and Class Members</u>

31. According to Avis's Notice, it learned of unauthorized access to its computer systems on August 5, 2024, with such unauthorized access having taken place between August 3, 2024, and August 6, 204.

[5] *Id.*

32. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including credit card numbers and expiration dates, dates of birth, and driver's license numbers.

33. On or about September 4, 2014, began to notify customers that its investigation determined that their Private Information was obtained.

34. Avis delivered Data Breach Notification Letters to Plaintiffs and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "data security incident."

35. The notice letter then attached some pages entitled "Attachment A" and "Attachment B – More Information about Identity Protection," which listed generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing one year of crediting monitoring that Plaintiffs and Class Members would have to affirmatively sign up for and a call center number that victims could contact "with any questions," Avis offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves. On information and belief, Avis sent a similar generic letter to all individuals affected by the Data Breach.

36. Avis had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

37. Plaintiffs and Class Members provided their Private 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 and to provide timely notice of any security breaches.

38. Avis's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

39. Avis knew or should have known that its electronic records would be targeted by cybercriminals.

C. Avis Failed to Comply with FTC Guidelines

40. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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. Indeed, the 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 Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

41. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

42. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. As evidenced by the Data Breach, Avis failed to properly implement basic data security practices. Avis's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

45. Avis was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from its failure to do so.

D. Avis Failed to Comply with Industry Standards

46. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

47. Some industry best practices that should be implemented by businesses like Avis include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor

authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

48. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

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

50. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Avis Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

51. In addition to its obligations under federal and state laws, Avis owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Avis owed a duty to Plaintiffs and Class Members to provide reasonable security, including complying with industry

standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

52. Avis breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Avis's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

53. Avis negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

54. Had Avis remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field,

it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

55. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Avis.

F. Avis Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

56. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[6] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

57. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal 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 or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

[6] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Sept. 17, 2024).

58. 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 to 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.

59. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

60. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

61. One such example of this is the development of "Fullz" packages.

62. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

63. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

64. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[7] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

65. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone fraud, bank fraud, or to obtain a driver's license or official identification card in the victim's name but with the thief's picture.

66. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the

[7] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Sept. 17, 2024).

consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

67. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[8] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry.

68. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[10]

69. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks.

---

[8] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on Sept. 17, 2024).

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Sept. 17, 2024).

[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on Sept. 17, 2024).

This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[11]

70. The Dark Web Price Index of 2022, published by PrivacyAffairs[12] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

71. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

72. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including Avis collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[13]

[11] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Sept. 17, 2024).

[12] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on Sept. 17, 2024).

[13] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Sept. 17, 2024).

73. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[14]

74. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

75. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

76. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

77. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[15]

> [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

[14] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).
[15] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Sept. 17, 2024).

> 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.

78. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

79. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiffs' and Class Members' Damages

Plaintiff Brooke Pestano's Experience

80. When Plaintiff Pestano first became a customer, Avis required Plaintiff Pestano provide it with substantial amounts of her PII.

81. On or about September 4, 2024, Plaintiff Pestano received a letter entitled "Notice of Data Breach" 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.

82. The notice letter offered Plaintiff Pestano only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Pestano will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

83. Plaintiff Pestano suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

84. Plaintiff Pestano would not have provided her Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard its customers personal information from theft, and that those systems were subject to a data breach.

85. Plaintiff Pestano suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

86. Plaintiff Pestano suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff Pestano entrusted to Defendants for the purpose of receiving rental car services from Defendants and which was compromised in, and as a result of, the Data Breach.

87. Plaintiff Pestano suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

88. Plaintiff Pestano has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

89. As a result of the Data Breach, Plaintiff Pestano made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendants, as well as long-term credit monitoring options she will now need to use. Plaintiff Pestano has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

90. As a result of the Data Breach, Plaintiff Pestano has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed

would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and other crimes against her. Plaintiff Pestano is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

91. Plaintiff Pestano also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendants obtained from Plaintiff Pestano; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

92. As a result of the Data Breach, Plaintiff Pestano anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Jennifer Signorile's Experience

93. When Plaintiff Signorile first became a customer, Avis required Plaintiff Signorile provide it with substantial amounts of her PII.

94. On or about September 4, 2024, Plaintiff Signorile received a letter entitled "Notice of Data Breach" 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, date of birth, and phone number.

95. The notice letter offered Plaintiff Signorile only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Signorile will now

experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

96. Plaintiff Signorile suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

97. Plaintiff Signorile would not have provided her Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard its customers' personal information from theft, and that those systems were subject to a data breach.

98. Plaintiff Signorile suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

99. Plaintiff Signorile suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff Signorile entrusted to Defendants for the purpose of receiving car rental services from Defendants and which was compromised in, and as a result of, the Data Breach.

100. Plaintiff Signorile suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

101. Plaintiff Signorile has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

102. As a result of the Data Breach, Plaintiff Signorile made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and

researching the credit monitoring offered by Defendants, as well as long-term credit monitoring options she will now need to use. Plaintiff Signorile has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

103. As a result of the Data Breach, Plaintiff Signorile has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and other crimes against her. Plaintiff Signorile is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

104. Plaintiff Signorile also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendants obtained from Plaintiff Signorile; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

105. As a result of the Data Breach, Plaintiff Signorile anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

106. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

107. Plaintiffs and Class Members entrusted their Private Information to Defendants in order to receive Defendants' services.

108. Plaintiffs' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices.

109. As a direct and proximate result of Avis's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having credit card accounts opened in their names, and other forms of identity theft.

110. Further, as a direct and proximate result of Avis's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

111. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

112. The Private Information maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

113. Plaintiffs and Class Members also lost the benefit of the bargain they made with Avis. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiffs and Class Members paid to Avis was intended to be used by Avis to fund adequate security of Avis's system and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class did not receive what they paid for.

114. Additionally, as a direct and proximate result of Avis's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

115. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

116. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[16] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[17]

117. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and

[16] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Sept. 17, 2024).

[17] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Sept. 17, 2024).

the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

118. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiffs and Avis included Avis's contractual obligation to provide adequate data security, which Avis failed to provide. Thus, Plaintiffs and Class Members did not get what they bargained for.

119. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

g. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

120. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Avis, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

121. As a direct and proximate result of Avis's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

122. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

123. Specifically, Plaintiffs propose the following Nationwide Class, as well as the following State Subclass definitions (also collectively referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

Illinois Subclass

All residents of Illinois who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

Florida Subclass

All residents of Illinois who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach

124. Excluded from the Class are Avis and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

125. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well as the Illinois and Florida Subclasses, before the Court determines whether certification is appropriate.

126. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

127. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 299,006 customers of Avis whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Avis's records, Class Members' records, publication notice, self-identification, and other means.

128. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Avis engaged in the conduct alleged herein;

b. Whether Avis's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act and/or Florida Unfair and Deceptive Trade Practices Act invoked below;

c. When Avis learned of the Data Breach;

d. Whether Avis's response to the Data Breach was adequate;

e. Whether Avis unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

f. Whether Avis failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Avis's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Avis's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Avis owed a duty to Class Members to safeguard their Private Information;

j. Whether Avis breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Avis had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether Avis breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether Avis knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Avis's misconduct;

p. Whether Avis's conduct was negligent;

q. Whether Avis's conduct was *per se* negligent;

r. Whether Avis was unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

129. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

130. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

131. Predominance. Avis has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Avis's conduct affecting Class Members set out above predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

132. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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, conducting 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.

133. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Avis has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

134. Finally, all members of the proposed Class are readily ascertainable. Avis has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Avis.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the State Subclasses)

135. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

136. Avis knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

137. Avis knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Avis was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

138. Avis owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Avis's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA and Illinois and Florida consumer protection laws;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

139. Avis's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

140. Defendants' duty also arose because Defendants were bound by industry standards to protect their customers' confidential Private Information.

141. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and Avis owed them a duty of care to not subject them to an unreasonable risk of harm.

142. Avis, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Avis's possession.

143. Avis, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

144. Avis, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

145. Avis breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

146. Avis had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Avis with their Private Information was predicated on the understanding that Avis would take adequate security precautions. Moreover, only Avis had the ability to protect its systems (and the Private Information that it stored on them) from attack.

147. Avis's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated as alleged herein.

148. Avis's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

149. As a result of Avis's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

150. Avis also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

151. As a direct and proximate result of Avis's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

152. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

153. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

154. 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 II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the State Subclasses)

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

156. Pursuant to Section 5 of the FTCA, Avis had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

157. Avis breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

158. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect.

159. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Avis's duty in this regard.

160. Avis violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

161. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Avis's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

162. Avis's violations of the FTCA constitute negligence *per se*.

163. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Avis's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

164. As a direct and proximate result of Avis's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

165. Avis breached its duties to Plaintiffs and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

166. As a direct and proximate result of Avis's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

167. 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 III
BREACH OF CONTRACT
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the State Subclasses)

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

169. 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.

170. 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 manner in which it became part of the agreement for services.

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

172. Plaintiffs and Class Members fully performed their obligations under their contracts with Avis.

173. 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.

174. 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.

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

176. 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.

177. 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.

178. 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
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the State Subclasses)

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

180. This Count is pleaded in the alternative to Count III above.

181. Avis provides rental car services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendants regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services from Defendants.

182. Through Avis's sale of services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with Avis's policies, practices, and applicable law.

183. As consideration, Plaintiffs and Class Members paid money to Avis and turned over valuable Private Information to Avis. Accordingly, Plaintiffs and Class Members bargained with Avis to securely maintain and store their Private Information.

184. Avis accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

185. In delivering their Private Information to Avis and paying for services, Plaintiffs and Class Members intended and understood that Avis would adequately safeguard the Private Information as part of that service.

186. Defendants' implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

187. Plaintiffs and Class Members would not have entrusted their Private Information to Avis in the absence of such an implied contract.

188. Had Avis disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Avis.

189. Avis recognized that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

190. Avis violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

191. Plaintiffs and Class Members have been damaged by Avis's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

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

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

193. This Count is pleaded in the alternative to Counts III and IV above.

194. Plaintiffs and Class Members conferred a benefit on Defendants by turning over their Private Information to Defendants and by paying for services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

195. Upon information and belief, Avis funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs and Class Members.

196. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Avis.

197. Avis has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

198. Avis knew that Plaintiffs and Class Members conferred a benefit upon it, which Avis accepted. Avis profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

199. If Plaintiffs and Class Members had known that Defendants had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendants.

200. Due to Avis's conduct alleged herein, it would be unjust and inequitable under the circumstances for Avis to be permitted to retain the benefit of its wrongful conduct.

201. As a direct and proximate result of Avis's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control 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 remains in Avis's possession and is subject to further unauthorized disclosures so long as Avis fails to undertake appropriate and adequate measures to protect Private Information in its 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 Plaintiffs and Class Members.

202. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Avis and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Avis from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

203. Plaintiffs and Class Members may not have an adequate remedy at law against Avis, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

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

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

205. 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).

206. 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).

207. 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 Class; (iii) failing to disclose or omitting materials 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.

208. 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.

209. 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.

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

211. 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.

212. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff and the Illinois Subclass have suffered harm: (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.

213. 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 VII
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)

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

215. Fla. Stat. § 501.201, *et seq.* is expressly intended to protect consumers like Plaintiff and Florida Subclass members from unfair or deceptive trade practices.

216. 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.

217. 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.

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

219. 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.

220. 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.

221. 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.

222. 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.

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

224. 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.

225. 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).

226. 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 of a substantial and imminent risk of future identity theft

for Plaintiff and the Florida Subclass.

227. 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 as a result of the loss of their financial and Private Information to third parties, as well as the steps victims should take to protect themselves.

228. 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.

229. 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.

230. 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.

231. 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.

232. Under FDUPTA, 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.

233. Avis's conduct in violation of FDUPTA 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.

234. 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 VIII
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class)

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

236. 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 to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described in this Complaint.

237. Avis owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

238. Avis still possesses Private Information regarding Plaintiffs and Class Members.

239. Plaintiffs allege that Avis's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

240. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Avis owes a legal duty to secure its customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. Avis's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' Private Information; and

c. Avis continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

241. This Court should also issue corresponding prospective injunctive relief requiring Avis to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order Avis to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Avis must implement and maintain reasonable security measures, including, but not limited to:

i. engaging 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 Avis to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Avis's systems;

v. conducting regular database scanning and security checks;

vi. 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; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps Avis's customers should take to protect themselves.

242. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Avis. The risk of another such breach is real, immediate, and substantial. If another breach at Avis occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

243. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Avis if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Avis's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Avis has a pre-existing legal obligation to employ such measures.

244. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at

Avis, thus preventing future injury to Plaintiffs and other customers whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and the State Subclasses requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Avis to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Avis to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: September 17, 2024.

Respectfully submitted,

/s/ David J. 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

Public court record.

This copy was downloaded from https://storage.courtlistener.com/recap/gov.uscourts.njd.554673/gov.
on 2026-10-19 and is hosted, unaltered, for reference at
https://chimo.ai/class-action/avis

Court: United States District Court for the District of New Jersey
Case number: 2:24-cv-09243-JXN-MAH
Filed: 2024-09-18

Chimo hosts public court records for readers' reference; documents are
unaltered copies from the court docket or the court-approved settlement website.