Adam Pollock
POLLOCK COHEN LLP
111 Broadway, Suite 1804
New York, NY 10006
(212) 337-5361

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
(312) 621-2000

*pro hac vice forthcoming

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

MAUREEN WRIGHT and DONALD WRIGHT, individually and on behalf of all others similarly situated, Plaintiffs, v. THE PRUDENTIAL INSURANCE COMPANY OF AMERICA, Defendant.	Case No. _____ CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Maureen Wright and Donald Wright ("Plaintiffs"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this Class Action Complaint against Defendant The Prudential Insurance Company of America ("Prudential" or "Defendant"), and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Prudential for its failure to secure and safeguard their and approximately 2,556,208 other individuals' personally identifying information ("PII") including, but not limited to, names, driver's license numbers, addresses, dates of birth, emails, and policy numbers.

2. Prudential is a large insurance and financial company that operates throughout the United States.

3. On or about February 5, 2024, Prudential discovered that an unauthorized third party had gained access to its network system and accessed and removed files containing information about Prudential's customers (the "Data Breach"). Despite Prudential knowing about the Data Breach on February 5, 2024, many customers first learned of the Data Breach in late-June or July of 2024, when they received a letter from Prudential notifying them of the Data Breach.

4. Prudential owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Prudential breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its customers' PII from unauthorized access and disclosure.

5. As a result of Prudential's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose

PII was exposed as a result of the Data Breach, which Prudential says it learned of on or about February 5, 2024.

6. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, negligence per se, breach of implied contract, unjust enrichment, and violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Maureen Wright

7. Plaintiff Maureen Wright ("Plaintiff M. Wright") is a citizen of Pennsylvania.

8. Plaintiff M. Wright obtained insurance services from Prudential. As a condition of receiving services, Prudential required Plaintiff M. Wright to provide it with her PII.

9. Based on representations made by Prudential, Plaintiff M. Wright believed Prudential had implemented and maintained reasonable security and practices to protect her PII. With this belief in mind, Plaintiff M. Wright provided her PII to Prudential in connection with receiving insurance services provided by Prudential.

10. At all relevant times, Prudential stored and maintained Plaintiff M. Wright's PII on its network systems.

11. Had Plaintiff M. Wright known that Prudential does not adequately protect the PII in its possession, she would not have obtained services from Prudential or agreed to entrust it with her PII.

12. Plaintiff M. Wright received a letter from Prudential dated June 24, 2024, which notified her that her PII was affected in the Data Breach.

13. As a direct result of the Data Breach, Plaintiff M. Wright has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII; deprivation of the value of her PII; and overpayment for services that did not include adequate data security.

Plaintiff Donald Wright

14. Plaintiff Donald Wright ("Plaintiff D. Wright") is a citizen of Pennsylvania.

15. Plaintiff D. Wright obtained insurance services from Prudential. As a condition of receiving services, Prudential required Plaintiff D. Wright to provide it with his PII.

16. Based on representations made by Prudential, Plaintiff D. Wright believed Prudential had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff D. Wright provided his PII to Prudential in connection with receiving insurance services provided by Prudential.

17. At all relevant times, Prudential stored and maintained Plaintiff D. Wright's PII on its network systems.

18. Had Plaintiff D. Wright known that Prudential does not adequately protect the PII in its possession, he would not have obtained services from Prudential or agreed to entrust it with his PII.

19. Plaintiff D. Wright received a letter from Prudential dated June 24, 2024, which notified him that his PII was affected in the Data Breach.

20. As a direct result of the Data Breach, Plaintiff D. Wright has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

Defendant The Prudential Insurance Company of America

21. Defendant The Prudential Insurance Company of America is a New Jersey corporation with its principal place of business located at 751 Broad Street, Newark, New Jersey, 07102.

JURISDICTION AND VENUE

22. The Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

23. This Court has general personal jurisdiction over Prudential because Prudential maintains its principal place of business in this District.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Prudential's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of Prudential

25. Prudential is a company that provides life insurance, investment, retirement, and other services.[1] The company has offices throughout the world.[2]

26. Prudential's website contains a Privacy Center, that states, "We maintain physical, electronic, and procedural safeguards to protect your personal information."[3] The Privacy Center contains a US Consumer Privacy Notice ("Privacy Notice"), which states, "We respect the privacy of your personal information and take our responsibility to protect it seriously."[4]

27. Prudential also maintains a HIPAA Notice of Privacy Practices, which it maintains for "[p]articipants of the Prudential Long-Term Care Insurance Plan and the Prudential Individual Health Plan."[5] The HIPAA Notice states, among other things, "We will not use or share your information other than as described in this Notice unless you tell us we can in writing."[6]

28. Prudential's website also contains a Data Security Statement that states, among other things, that "Prudential regularly faces cybersecurity threats and attempted attacks, both general and targeted, against our operating environment," and

---

[1] Prudential, https://www.prudential.com/.
[2] *Worldwide Locations*, PRUDENTIAL, https://www.prudential.com/links/about/worldwide-locations/.
[3] *Privacy Center*, PRUDENTIAL, https://www.prudential.com/links/privacy-center.
[4] *Privacy Policy*, PRUDENTIAL, https://www.prudential.com/links/privacy-policy.
[5] *HIPAA Notice of Privacy Practices*, PRUDENTIAL, https://www.prudential.com/links/hipaa.
[6] *Id.*

"[p]rotecting the data entrusted to us, especially personal data, and protecting our operating environment remain top areas of focus for Prudential."[7]

29. Plaintiffs and Class members are customers of Prudential and entrusted Prudential with their PII.

The Data Breach

30. On or about February 5, 2024, Prudential discovered "unauthorized third-party access to certain company systems and data."[8] After an investigation, Prudential determined that "the unauthorized third party gained access to [its] network on February 4, 2024," and that PII was removed from the system.[9]

31. The letters that Prudential sent to Plaintiffs state that the Data Breach affected Plaintiffs' "name, address, date of birth, email, and policy number." Previous reports stated that the Data Breach also included "driver's license numbers" and "non-driver identification card numbers." [10]

32. The Alphv/BlackCat ransomware group has claimed that it was responsible for the attack on Prudential and listed the attack on its leak site.[11]

---

[7] *Data Security Statement*, PRUDENTIAL, https://www.prudential.com/links/about/data-security-statement.
[8] *Notice Letter*, PRUDENTIAL, https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/bcc5d2ac-a40f-4204-89ca-4b665f43c362/8b2e3c35-6dc8-4bc3-b4d4-86c55b63e716/Individual%20Notification%20Letter%20Template%20(3.29.2024).PDF.
[9] *Id.*
[10] Ionut Arghire, SECURITYWEEK (Apr. 2, 2024), https://www.securityweek.com/36000-impacted-by-prudential-financial-data-breach/.
[11] *Id.*

Prudential Knew that Criminals Target PII

33. At all relevant times, Prudential knew, or should have known, that the PII that it collected and stored was a target for malicious actors. Indeed, Prudential was clearly aware of the threat of a data breach, as it states in its Data Security Statement that "Prudential regularly faces cybersecurity threats and attempted attacks … ."[12]

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

35. It is well known amongst companies that store sensitive personally identifying information that sensitive information is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers … . Many of them were caused by flaws in … systems either online or in stores."[13]

36. PII is a valuable property right.[14] The value of PII as a commodity is measurable.[15] "Firms are now able to attain significant market valuations by employing

---

[12] *Data Security Statement*, *supra* note 7.

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

[14] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

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

business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[17] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

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

38. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[18]

39. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the

---

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

[17] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[18] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[19]

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

Theft of PII Has Grave and Lasting Consequences for Victims

41. Theft of PII can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[20, 21]

42. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[22]

---

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

[20] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft.

[21] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[22] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023),

43. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[23]

44. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[24]

45. It is within this context that Plaintiffs and Class members must now live with the knowledge that their PII is forever in cyberspace, having been stolen by criminals willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Damages Sustained by Plaintiffs and Class Members

46. Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which

---

https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[23] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/.

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

remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

47. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

48. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

> All United States residents whose personally identifiable information was accessed by and disclosed in the Data Breach to unauthorized persons, including all who were sent a notice of the Data Breach.

49. Excluded from the Class is The Prudential Insurance Company of America, and its affiliates, parents, subsidiaries, employees, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

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

51. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. Prudential has reported that the Data Breach affected approximately 2,556,210 persons.[25]

[25] *Data Breach Notifications*, Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/cc7a25d8-bb55-485b-b3bc-060aa12004dd.html.

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

a. whether Prudential had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII from unauthorized access and disclosure;

b. whether Prudential had duties not to disclose the PII of Plaintiffs and Class members to unauthorized third parties;

c. whether Prudential failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII;

d. whether an implied contract existed between Class members and Prudential, providing that Prudential would implement and maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;

e. whether Prudential engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class members;

f. whether Prudential breached its duties to protect Plaintiffs' and Class members' PII; and

g. whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

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

54. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions

committed by Prudential, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

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

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

CAUSES OF ACTION

COUNT I
NEGLIGENCE

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

58. Prudential owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting the PII in its possession, custody, or control.

59. Prudential knew or should have known the risks of collecting and storing Plaintiffs' and all other Class members' PII and the importance of maintaining secure systems. Prudential knew or should have known of the many data breaches that targeted companies that collect and store PII in recent years.

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

61. Prudential breached its duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiffs' and Class members' PII.

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

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

64. As a result of Prudential's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Prudential's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the compromise of their PII as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

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

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

67. Prudential violated Section 5 of the FTCA, by failing to use reasonable measures to protect Plaintiffs' and other Class members' PII, by failing to provide timely notice, and by not complying with applicable industry standards. Prudential's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

68. Prudential's violation of Section 5 of the FTCA constitutes negligence per se.

69. Plaintiffs and Class members are within the class of persons that Section 5 of the FTCA is intended to protect.

70. The harm occurring as a result of the Data Breach is the type of harm that Section 5 of the FTCA is intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and Class members as a result of the Data Brach.

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

72. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Prudential's violations of Section 5 of the FTCA. Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Prudential's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the compromise of their PII as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT

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

74. In connection with receiving insurance or other services, Plaintiffs and all other Class members entered into implied contracts with Prudential.

75. Pursuant to these implied contracts, Plaintiffs and Class members paid money to Prudential and provided Prudential with their PII. In exchange, Prudential agreed to, among other things, and Plaintiffs understood that Prudential would: (1) provide services to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and

(3) protect Plaintiffs' and Class members' PII in compliance with federal and state laws and regulations and industry standards.

76. The protection of PII was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Prudential, on the other hand. Indeed, as set forth *supra*, Prudential recognized the importance of data security and the privacy of its clients' PII in its Privacy Notice. Had Plaintiffs and Class members known that Prudential would not adequately protect its clients' PII, they would not have received insurance or other services from Prudential.

77. Plaintiffs and Class members performed their obligations under the implied contract when they provided Prudential with their PII and paid for services from Prudential.

78. Prudential breached its obligations under its implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

79. Prudential's breach of its obligations of its implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

80. Plaintiffs and all other Class members were damaged by Prudential's breach of implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk

justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) they overpaid for services that were received without adequate data security.

COUNT IV
UNJUST ENRICHMENT

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

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

83. Plaintiffs and Class members conferred a monetary benefit upon Prudential in the form of monies paid for services and through the provision of their PII.

84. Prudential accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Prudential also benefitted from the receipt of Plaintiffs' and Class members' PII, as this was used to facilitate billing services.

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

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

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

88. Prudential should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW ("UTPCPL")
73 P.S. §§ 201-1–201-9.3

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

90. Prudential performs services in the Commonwealth of Pennsylvania.

91. Plaintiffs, Class members, and Prudential are "persons" as defined by the UTPCPL. 73 P.S. § 201-2(2).

92. Prudential's insurance and other services constitute "trade" and "commerce" under the statute. 73 P.S. § 201-2(3).

93. Prudential obtained Plaintiffs' and Class members' PII in connection with the insurance and other services that Prudential performed.

94. Prudential engaged in unfair or deceptive acts in violation of the UTPCPL by failing to implement and maintain reasonable security measures to

protect and secure its customers' PII in a manner that complied with applicable laws, regulations, and industry standards.

95. Prudential makes explicit statements to its customers that it will adequately safeguard their PII, as evidenced by its Privacy Notice, HIPAA Notice, and Data Security Statement.

96. The UTPCPL lists twenty-one instances of "unfair methods of competition" and "unfair or deceptive acts or practices." 73 P.S. § 201-2(4). Prudential's failure to adequately protect Plaintiffs and Class members' PII while holding out that it would adequately protect the PII falls under at least the following categories:

a. representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have, or that a person has a sponsorship, approval, status, affiliation or connection that he does not have (73 P.S. § 201-2(4)(v));

b. representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another (73 P.S. § 201-2(4)(vii));

c. advertising goods or services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)); and

d. engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

97. Due to the Data Breach, Plaintiffs and Class members have lost property in the form of their PII. Further, Prudential's failure to adopt reasonable practices in protecting and safeguarding its customers' PII will force Plaintiffs and Class members to spend time or money to protect against identity theft. Plaintiffs and Class members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Prudential's practice of

collecting and storing PII without appropriate and reasonable safeguards to protect such information.

98. As a result of Prudential's violations of the UTPCPL, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of, or imminent threat of, identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Prudential's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the compromise of their PII as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

99. Pursuant to 73 P.S. § 201-9.2(a), Plaintiffs seek actual damages, $100, or three times their actual damages, whichever is greatest. Plaintiffs also seek costs, expenses, and reasonable attorney fees.

PRAYER FOR RELIEF

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: July 10, 2024

Respectfully submitted,

/s/ Adam Pollock

Adam Pollock
POLLOCK COHEN LLP
111 Broadway, Suite 1804
New York, NY 10006
(212) 337-5361

adam@pollockcohen.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
(312) 621-2000
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiffs and the Proposed Class
**pro hac vice forthcoming*