Joseph J. DePalma
Catherine B. Derenze
LITE DEPALMA GREENBERG & AFANADOR, LLC
570 Broad Street, Suite 1201
Newark, NJ 07102
Tel: 973-623-3000
Fax: 973-623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

Attorneys for Plaintiffs and the Putative Class
[Additional Counsel Listed on Signature Page]

UNITED STATES DISTRICT COURT
DISTRICT COURT OF NEW JERSEY

IN RE: PRUDENTIAL FINANCIAL, INC. DATA BREACH LITIGATION,	Case No. 2:24-cv-06818
This Document Relates To:	CONSOLIDATED CLASS ACTION COMPLAINT
ALL ACTIONS	JURY DEMAND

Plaintiffs Connie Boyd, Gina Adinolfi, John Moss, Stephanie Demaro, Anthony Guissarri, and Roger Menhennett ("Plaintiffs") bring this class action, individually and on behalf of all others similarly situated ("Class Members"), against Defendant Prudential Financial, Inc. d/b/a The Prudential Insurance Company of America ("Prudential" or "Defendant") for its failure to properly secure and safeguard Plaintiffs' and Class Members' personally identifiable information ("PII") and personal health information ("PHI") stored within Defendant's information network, and allege as follows, based upon information and belief, investigation of counsel, and the personal knowledge of Plaintiffs.

I. INTRODUCTION

1. Prudential is a "financial service company based in Newark, New Jersey. Prudential provides retail and institutional clients with a range of services, including insurance, retirement

planning, investment management and more."[1]

2. During the regular course of conducting its business, Defendant acquired, collected, and stored customer PII and PHI (collectively "Private Information") for the purpose of providing products and services, including life insurance, health insurance, annuities, retirement-related services, mutual funds, and investment management.

3. Upon information and belief, on or about February 4, 2024, unauthorized third-party cybercriminals gained access to customer Private Information that Defendant was storing on its networks, with the intent of engaging in the misuse of the Private Information, including marketing and selling customer Private Information (hereinafter the "Data Breach").

4. On February 21, 2024, Prudential filed a notice with the U.S. Securities and Exchange Commission ("SEC") disclosing the cyber-attack:

> As disclosed in the Original Report, on February 5, 2024, we detected that, beginning February 4, 2024, a threat actor had gained unauthorized access to certain of our systems. With assistance from external cybersecurity experts, we immediately activated our cybersecurity incident response process to investigate, contain, and remediate the incident. As of the date of this Report, we believe the threat actor is a cybercrime group, and our investigation has identified that the group accessed and exfiltrated from a platform limited data that includes some client information and personally identifiable information. The threat actor also accessed and exfiltrated Company administrative and user data from certain information technology systems and accessed a small percentage of Company user accounts associated with employees and contractors. We reported this matter to relevant law enforcement and have been informing regulatory authorities.[2]

5. In total, cybercriminals exfiltrated the Private Information of 2,556,210 individuals due to Defendant's failure to implement appropriate data security safeguards to protect their customers' Private Information. [3]

---

[1] *See* https://www.jdsupra.com/legalnews/prudential-financial-confirms-february-7157159/ (last accessed on June 5, 2024).
[2] *See* https://www.sec.gov/ix?doc=/Archives/edgar/data/1137774/000119312524040749/d766318d8ka.htm (last accessed on June 5, 2024).
[3] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/cc7a25d8-bb55-485b-b3bc-060aa12004dd.html (last accessed on Oct. 9, 2024).

6. The exfiltrated Private Information at issue included but is not limited to: name, address, date of birth, email, phone number, Social Security numbers, health information, account and credit card numbers, and Prudential ID number.

7. Plaintiffs and Class Members are current and former customers, clients, and their beneficiaries, who provided their Private Information to Defendant directly or indirectly in connection with those products and services.

8. As further alleged herein, Defendant knew or should have known, that Plaintiffs and Class Members would use Defendant's services and benefits to store and/or share sensitive data, including highly confidential Private Information.

9. Moreover, Defendant knew or should have known that its customer Private Information was extremely valuable to cybercriminals given the dozens of recent cyberattacks targeting the healthcare industry and exfiltrating highly sensitive healthcare information.

10. Nevertheless, as further alleged herein, Plaintiffs' and Class Members' Private Information was compromised due to Defendant's negligent and/or reckless acts and omissions and Defendant's repeated failure to reasonably and adequately protect Plaintiffs' and Class Members' Private Information.

11. Accordingly, Plaintiffs and Class Members seek damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including reasonable and adequate improvements to Defendant's data security systems, policies, and practices, the implementation of annual audits reviewing the same, adequate credit monitoring services funded by Defendant, and payment for the costs of repairing damaged credit as a result of the Data Breach.

II. JURISDICTION AND VENUE

12. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction).

Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendant.

13. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367. Defendant is headquartered in New Jersey, and its principal place of business is located there. Prudential routinely conducts business in New Jersey, has sufficient minimum contacts in this state, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this state.

14. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiffs' claims occurred within this District, and Defendant does business in this Judicial District.

III. PARTIES

15. Plaintiff Connie Boyd is an adult individual and, at all relevant times herein, a resident and citizen of Minnesota, residing in Hinckley, Minnesota. Plaintiff is a client of Defendant and a victim of the Data Breach.

16. Plaintiff Gina Adinolfi is an adult individual and, at all relevant times herein, a resident and citizen of New Jersey, residing in Warren County, New Jersey. Plaintiff Adinolfi is a client of Defendant and a victim of the Data Breach.

17. Plaintiff John Moss is an adult individual and, at all relevant times herein, a resident and citizen of Pennsylvania, residing in Philadelphia County, Pennsylvania. Plaintiff is a client of Defendant and a victim of the Data Breach.

18. Plaintiff Stephanie Demaro is an adult individual and, at all relevant times herein, a resident and citizen of Pennsylvania, residing in Westmoreland County, Pennsylvania. Plaintiff Demaro is a client of Defendant and a victim of the Data Breach.

19. Plaintiff Anthony Guissarri is an adult individual and, at all relevant times herein, a resident and citizen of California, residing in Palm Springs, California. Plaintiff Guissarri is a client of Defendant and a victim of the Data Breach.

20. Plaintiff Roger Menhennett is an adult individual and, at all relevant times herein, a resident and citizen of New York, residing in Endicott, New York. Plaintiff Menhennett is a client of Defendant and a victim of the Data Breach.

21. Defendant Prudential Financial, Inc., is a New Jersey corporation headquartered at 751 Broad Street, Newark, New Jersey 07102.

IV. FACTUAL ALLEGATIONS OF DEFENDANT'S CONDUCT

A. The Data Breach

22. Beginning on or around February 4, 2024, Defendant was subjected to a cyberattack which compromised the sensitive Private Information of Plaintiffs and Class Members.

23. In a Form 8-K filed with the SEC, Prudential noted that it learned on February 5, 2024, that a threat actor had "gained unauthorized access" to Prudential's "administrative and user data from certain technology systems and a small percentage of Company users accounts associated with employees and contractors."[4]

24. Prudential's SEC notice also stated that Prudential was investigating the Data Breach:

> We continue to investigate the extent of the incident, including whether the threat actor accessed any additional information or systems, to determine the impact of the incident. On the basis of the investigation to date, we do not have any

[4] Prudential Financial, Inc., Form 8-K, United States Securities and Exchange Commission (Feb. 12, 2024).

> evidence that the threat actor has taken customer or client data. We have reported this matter to relevant law enforcement and are informing regulatory authorities.[5]

25. However, the SEC notice, dated February 12, 2024, did not state whether the threat actor still had unauthorized access to Prudential's systems.

26. In fact, on or about February 16, 2024, the cybercrime group "Blackcat" (also known as "ALPHV," referred to hereinafter as "ALPHV Blackcat") claimed credit on its darknet site for the attack and claimed that it still had access to Prudential's systems.[6]

27. ALPHV Blackcat is a notorious cybercriminal group. As of December 19, 2023, ALPHV Blackcat "ha[d] targeted the computer networks of more than 1,000 victims and caused harm around the world since its inception, including networks that support U.S. critical infrastructure."[7] The U.S. Department of Justice further noted that "has emerged as the second most prolific ransomware-as-a-service variant in the world based on the hundreds of millions of dollars in ransoms paid by victims around the world."[8]

28. ALPHV Blackcat is known for being the first ransomware to create a public data leaks website on the open internet. Previous cyber gangs typically published stolen data on the dark web. ALPHV BlackCat's innovation was to post excerpts or samples of victims' data on a site accessible to anyone with a web browser.

29. ALPHV Blackcat has targeted hundreds of organizations worldwide, including Reddit, MGM, and Caesars in 2023, and Change Healthcare in 2024.

30. As time progressed, Prudential revealed more and more of its customers and former

---

[5] *Id.*
[6] Eduard Kovacs, *Ransomware Group Takes Credit for LoanDepot, Prudential Financial Attacks*, SECURITYWEEK, (Feb. 19, 2024), https://www.securityweek.com/ransomware-group-takes-credit-for-loandepot-prudential-financial-attacks/.
[7] *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, U.S. Department of Justice, (Dec. 19, 2023) https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.
[8] *Id.*

customers, as well as their beneficiaries, had their Private Information exfiltrated by, upon information and belief, ALPHV Blackcat.

31. First, on Friday, March 29, 2024—the weekend of the Easter Holiday, Prudential filed a data breach notification with the Maine Attorney General that stated the personal information of 36,545 customers "related to [their] Prudential products and services," including name, address, driver's license number, and non-driver identification card number had been exfiltrated in the Data Breach.[9] The March 29, 2024 notice also finally confirmed that cybercriminals no longer "ha[d] access to [Prudential's] systems."[10]

32. Second, Prudential reported to the Secretary of the United States Department of Health and Human Services on April 22, 2024, that a "Hacking/IT Incident" of its "Network Server" resulted in the exposure of Private Information of 36,092 individuals.[11]

33. And third, on Friday, June 28, 2024, Prudential amended its notice of data breach with the Maine Attorney General's Office to reveal that the Data Breach actually had actually impacted 2,556,210 of its customers.[12] The filing did not state what categories of personal information had been exfiltrated by cybercriminals;[13] however, in a filing on the same date with the Office of the Attorney General of Iowa, Prudential revealed the affected customer information included: Social Security number, credit and debit card information, financial account information, driver's license, treatment, diagnosis and prescription information, and health condition

[9] *Data Breach Notifications*, Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/2605118e-36eb-44d8-933a-2e084c069f84.shtml (Mar. 29, 2024).
[10] *Id.*
[11] U.S. Department of Health and Human Services, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed July 10, 2024).
[12] *Data Breach Notifications*, Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/cc7a25d8-bb55-485b-b3bc-060aa12004dd.html (June 28, 2024).
[13] *Id.*

information.[14]

B. Defendant's Failed Response to the Breach

34. Prudential's investigation determined that Plaintiffs' and Class Members' Private Information was compromised in the Data Breach. Specifically, Prudential's investigation discovered that the Private Information of Plaintiffs' and Class Members', including their first name, last name, date of birth, policy numbers, addresses, email addresses, phone numbers, Social Security numbers, credit card information, debit card information, financial account information, driver's license information, health treatment information, health diagnosis information, prescription information, and health condition information, had been compromised.

35. Yet, Prudential waited almost *two months* after it initially discovered the Data Breach to begin notifying affected individuals and, to date, has not indicated whether it completed the notification process as Prudential has been notifying affected individuals on a "rolling basis."

36. Beginning in late March, Prudential sent Plaintiffs and other Class Members a Data Breach Notice, which said the following:

> **What Happened?**
>
> On February 5, 2024, Prudential detected unauthorized third-party access to certain company systems and data. We promptly activated our incident response plan and launched an investigation into the nature and scope of the issue with assistance from external cybersecurity experts. We also reported this matter to relevant law enforcement. Through the investigation, we learned that the unauthorized third party gained access to our network on February 4, 2024 and removed a small percentage of personal information from our systems.

37. Omitted from the Data Breach Notice is information explaining the root cause of the Data Breach, the vulnerabilities exploited by the cybercriminals, and Defendant's prior data

[14] *Data Breach Notice*, Iowa Attorney General, https://www.iowaattorneygeneral.gov/media/cms/6282024_Prudential_Insurance_Compan_ED906E8233AB8.pdf (June 28, 2024).

breach history and efforts to ensure similar breaches did not continue to occur, exposing customers' Private Information. To date, these omitted details have not been explained or revealed to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is not repeatedly exposed to cybercriminals by Defendant.

38. Upon information and belief, the unauthorized third-party cybercriminals specifically targeted Defendant based on its status as an insurer, financial services and product provider, which has enormous amounts of valuable Private Information—including the Private Information of Plaintiffs and Class Members. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' Private Information with the intent of engaging in the misuse of the Private Information, including marketing and selling Plaintiffs' and Class Members' Private Information.

39. Defendant had and continues to have obligations under applicable federal and state laws as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiffs' and Class Members' Private Information confidential and to protect such Private Information from unauthorized access.

40. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a result of their dealings. In furtherance of this relationship, Defendant created, collected, and stored Plaintiffs' and Class Members' Private Information with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

41. Despite this, Plaintiffs and Class Members remain, even today, in the dark regarding what data was stolen, the particular malware used, and what steps were and are being taken to secure their Private Information going forward.

42. Plaintiffs and Class Members are, thus, left to speculate as to where their Private Information ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

43. Plaintiffs' and the Class Members' Private Information is, upon information belief, up for sale on the dark web and potentially in the hands of companies that will use the detailed Private Information for targeted marketing without Plaintiffs' and/or Class Members' approval. Either way, unauthorized individuals can now easily access Plaintiffs' and Class Members' Private Information.

C. Defendant Collected/Stored Class Members' Private Information

44. Defendant is a financial services and investment manager with approximately $1.551 trillion of assets under management as of March 31, 2024, and has operations in the United States, Asia, Europe, and Latin America.[15]

45. Defendant offers a wide array of products and services, including life insurance, health insurance, annuities, retirement-related services, mutual funds, and investment management.

46. While providing its customers with products and services, Defendant receives, creates, handles, and transfers its customers' Private Information.

47. As a condition of its relationships with Plaintiffs and Class Members, Defendant required that Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential Private Information, including some or all of the following:

a. Full names and addresses;

[15] Prudential Financial Inc., Form 8-K, United States Securities and Exchange Commission (July 2, 2024).

b. Personal email addresses and phone numbers;

c. Dates of birth;

d. Social Security numbers;

e. Driver's licenses (or similar state identifications);

f. Health information including, but not limited to, information about diagnosis, treatment, prescriptions, and health conditions; and

g. Information related to credit and debit card numbers, bank account statements and financial account details.

48. Defendant, in turn, stored that Private Information in the part of Defendant's system that was ultimately affected by the Data Breach.

49. This type of Private Information is extremely sensitive and extremely valuable to criminals because it can be used to commit serious identity and medical identity theft crimes.

50. Upon information and belief, Defendant promised to, among other things: keep Private Information private; comply with healthcare insurance industry standards related to data security and Private Information, including FTC and HIPAA guidelines; inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Plaintiffs and Class Members obtain from Defendant and provide adequate notice to individuals if their Private Information is disclosed without authorization.

51. By obtaining, collecting, and storing Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

52. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

53. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

54. Defendant could have prevented the Data Breach, which began no later than February 4, 2024, by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiffs' and Class Members' Private Information.

D. The Data Breach Was Foreseeable

55. The Data Breach was entirely foreseeable and avoidable.

56. First, this Data Breach is not the only data breach Defendant suffered in the span of a year. In July 2023, Defendant experienced another data breach that exposed the Private Information of 320,840 individuals, including their Social Security numbers.[16]

57. Second, Defendant's negligence in safeguarding Plaintiffs' and Class Members' Private Information is exacerbated by repeated warnings and alerts directed at protecting and securing sensitive data, as evidenced by recent trending data breach attacks.

58. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and the U.S. Secret Service have warned potential targets so they are aware of, can prepare for, and hopefully ward off a potential attack.

59. And third, Defendant is a health insurer handling medical information. Thus, Defendant's data security obligations were particularly important given the substantial increase in

[16] *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/e2a5ab4c-3947-4a2e-a9fe-b58eec80686c.shtml (last visited July 10, 2024).

cyberattacks and data breaches in the healthcare industry and other industries which held significant amounts of Private Information preceding the Data Breach.

60. Although Defendant knew or should have known that Plaintiffs' and Class Members' Private Information was a target for malicious actors, Defendant failed to take appropriate steps to protect Plaintiffs' and Class Members' Private Information from being compromised.

E. Defendant Had an Obligation to Protect the Stolen Information

61. In failing to secure Plaintiffs' and Class Members' sensitive data adequately, Defendant breached duties it owed Plaintiffs and Class Members under statutory and common law. Moreover, Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also had an implied duty to safeguard its data, independent of any statute.

62. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce."[17]

63. According to the FTC, data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Private Information.

64. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and

[17] The Federal Trade Commission (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 the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

practices for business. The guidelines explain that companies should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of Private Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems

65. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

66. The FTC recommends that companies not maintain information longer than is necessary 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 for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

67. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

68. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

69. Defendant also failed to comply with their obligations under the Health Insurance

Portability and Accountability Act of 1996 ("HIPAA").

70. As a health plan handling medical patient data, Defendant is a covered entity under HIPAA (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

71. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

72. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

73. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information that is kept or transferred in electronic form.

74. The Data Breach is considered a breach under the HIPAA Rules because it involved access to PHI not permitted under the HIPAA Privacy Rule.

75. A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

76. The Data Breach resulted from multiple failures by Defendant to adequately and reasonably secure Plaintiffs' and Class Members' Private Information in violation of the mandates set forth in HIPAA's regulations.

77. As a covered entity, Defendant is required under federal and state law to maintain

the strictest confidentiality of the PHI it acquires, receives, collects, transfers, and stores. Defendant is further required to maintain sufficient safeguards to protect that PHI from being accessed by unauthorized third parties and to ensure the confidentiality, integrity, and availability of PHI. These safeguards include physical, technical, and administrative components.

78. Due to the nature of Defendant's insurance businesses, which include providing insurance for individuals in need of long-term care such as nursing homes, assisted living, and a home health aide,[18] and providing individual health insurance plans,[19] Defendant would be unable to engage in its regular business activities without collecting and aggregating PHI it knows and understands to be sensitive and confidential.

79. As Prudential acknowledges in its "HIPAA Notice of Privacy Practices," HIPAA requires that Defendant use adequate safeguards to prevent unauthorized use or disclosure of PHI, including by implementing the HIPAA Security Rule and immediately report any unauthorized use or disclosure of PHI (such as the Data Breach) to affected individuals.[20]

80. For its part, Defendant explicitly touted its commitment to protecting the privacy of Private information for its insurance-related products and services as well as its financial products and services, including life insurance, annuities, retirement-related services, mutual funds, and investment management, claiming that:

> Prudential values your business and your trust. We respect the privacy of your personal information and take our responsibility to protect it seriously. This privacy notice is provided on behalf of the Prudential companies . . . and applies to our current and former customers.

---

[18] Prudential, *Long-Term Care: What to Know and How to Plan*, PRUDENTIAL, https://www.prudential.com/financial-education/understanding-long-term-care (last accessed July 10, 2024).

[19] Prudential, *Affordable Individual Health Insurance Plans*, https://www.prudential.com/wps/portal/production/prudential/personal/health-insurance (last accessed July 10, 2024).

[20] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. See 45 C.F.R. Part 160 and Part 164, Subparts A and C

. . . .

> We maintain physical, electronic, and procedural safeguards to protect your personal information. The people authorized to access your personal information need it to do their jobs, and we require that they keep your information secure and confidential.[21]

Likewise, in its "Online Privacy Statement," Prudential promises:

> **Social Security Numbers**
> Prudential collects Social Security numbers in the course of its business activities. Prudential has a privacy policy that is designed to protect personal information, including Social Security numbers. This policy requires that Prudential have measures in place to keep all personal information about its customers and employees, and employees of our vendors and business partners, secure and confidential.
>
> **Retention Period**
> Prudential retains personal information for as long as needed or permitted in light of the purpose(s) for which it was obtained and consistent with applicable law.
>
> . . . .
>
> **Security**
> Prudential seeks to use reasonable administrative, technical and physical safeguards and other security measures to protect personal information within our organization.[22]

81. Prudential also states in its "Online Privacy Statement" that it uses Plaintiffs' and Class Members' Private Information to provide its customers "tailored content and marketing messages;" "operate, evaluate, and improve our business (including developing new products and services; improving existing products, services and Online Services; performing data analytics; and performing accounting, auditing, and other internal functions;" and "manage infrastructure and other business operations."[23]

---

[21] *US Consumer Privacy Notice*, PRUDENTIAL, https://www.prudential.com/links/privacy-policy (last accessed July 10, 2024).
[22] *Online Privacy Statement*, PRUDENTIAL, https://www.prudential.com/links/privacy-statement (last accessed July 10, 2024).
[23] *Id.*

82. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

83. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

84. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Plaintiffs and Class Members.

85. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the Private Information was adequately secured and protected.

86. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

87. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

88. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

89. Defendant owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust this Private Information to Defendant.

90. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

91. Defendant owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' Private Information and monitor user behavior and activity to identify possible threats.

92. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to safeguard Plaintiffs' and Class Members' Private Information adequately; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

93. Despite its duties under the law to Plaintiffs and Class Members to protect and safeguard their Private Information and the foreseeability of a data breach, Defendant failed to implement reasonable and adequate data security measures, directly resulting in the Data Breach.

94. Defendant owed a non-delegable duty to Plaintiffs and Class Members to implement reasonable and adequate security measures to protect their Private Information. Yet, Defendant maintained and shared the Private Information in a negligent and/or reckless manner.

In particular, Defendant failed to train its employees on proper cybersecurity measures adequately.

F. Value of the Relevant Sensitive Information

95. Private Information is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other Private Information on several underground internet websites. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

96. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[24]; Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[25]; and other sources report that criminals can also purchase access to entire company data breaches from $999 to $4,995.[26]

97. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[27] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[28] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[29]

98. The FTC defines identity theft as "a fraud committed or attempted using the

[24] *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 accessed Oct. 9, 2024).
[25] *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 accessed Oct. 9, 2024).
[26] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Oct. 9, 2024).
[27] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed Oct. 9, 2024).
[28] *Id.*
[29] *Id.*

identifying information of another person without authority." 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."

99. Identity thieves can use Private Information, such as that of Plaintiffs and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

100. There may be a time lag between when harm occurs versus when it is discovered and when Private Information is stolen and when it is used.

101. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

102. Here, Defendant knew of the value of Private Information and of the foreseeable consequences that would occur if Plaintiffs' and Class Members' Private Information were stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of

[30] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed June 5, 2024).

a breach of this magnitude.

103. As detailed above, Defendant is a sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiffs and Class Members. Therefore, its failure to do so is intentional, willful, reckless and/or grossly negligent.

104. Now armed with the Private Information accessed in the Data Breach, cybercriminals can use or sell the Private Information to further harm Plaintiffs and Class Members in a variety of ways including: destroying their credit by opening new financial accounts and taking out loans in Class Members' names; using Class Members' names to obtain medical services improperly; using Class Members' Private Information to target other phishing and hacking intrusions; using Class Members' Private Information to obtain government benefits; and otherwise assuming Class Members' identities.

105. As a result of the Data Breach, Plaintiffs and Class Members face a substantial and ongoing risk of imminent harm relating to the exposure and misuse of their Private Information. Plaintiffs and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

106. Plaintiffs and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages.

107. Despite this, Defendant has offered only a limited two-year subscription for identity

theft monitoring and identity theft protection. Its limitation is inadequate when the victims will likely face many years of identity theft.

V. PLAINTIFFS' COMMONFACTUAL ALLEGATIONS

A. Plaintiff Connie Boyd

108. Plaintiff Boyd's information was stored with Defendant as a result of her dealings with Defendant.

109. As required in order to obtain services from Defendant, Plaintiff Boyd provided Defendant with her Private Information, including but not limited to her name, date of birth, address, email address, Social Security number, account numbers, email, which Defendant then possessed and controlled.

110. As a result, Plaintiff Boyd's information was among the Private Information accessed by an unauthorized third-party in the Data Breach.

111. At all times herein relevant, Plaintiff Boyd is and was a member of the Class.

112. Plaintiff Boyd received a letter from Defendant, dated May 28, 2024, stating that her Private Information was involved in the Data Breach (the "Notice").

113. Plaintiff Boyd was unaware of the Data Breach until receiving the Notice.

114. As a result, Plaintiff Boyd was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring her accounts with heightened scrutiny and time spent seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach.

115. Plaintiff Boyd was also injured by the material risk to future harm she may suffer

based on Defendant's breach; this risk is imminent and substantial because Plaintiff Boyd's data has been exposed in the Data Breach, the data involved, including Social Security numbers, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

116. Plaintiff Boyd suffered actual injury in the form of damages to and diminution in the value of her Private Information —a condition of intangible property that she entrusted to Defendant, which was compromised in and as a result of the Data Breach.

117. Plaintiff Boyd, as a result of the Data Breach, has increased anxiety about her loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling her Private Information.

118. Plaintiff Boyd has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

119. Plaintiff Boyd has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

B. Plaintiff Gina Adinolfi

120. Plaintiff Adinolfi's information was stored with Defendant as a result of her dealings with Defendant.

121. As a condition of obtaining life insurance with Prudential, Plaintiff Adinolfi was required to provide her Private Information to Defendant, including her name, address, date of birth, and full health and financial information.

122. At the time of the Data Breach, Defendant stored and maintained Plaintiff

Adinolfi's Private Information.

123. Plaintiff Adinolfi is very careful about sharing her sensitive Private Information. Plaintiff Adinolfi stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Adinolfi would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

124. Plaintiff Adinolfi received the Notice Letter, by U.S. mail, directly from Defendant, dated May 28, 2024. According to the Notice Letter, Plaintiff Adinolfi's Private Information was improperly accessed and obtained by unauthorized third parties, including her name, address, date of birth, phone number, and Prudential ID number.

125. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Adinolfi made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring her own computer network, and contacting companies regarding suspicious activity on her accounts. Plaintiff Adinolfi has spent significant time dealing with the Data Breach—valuable time Plaintiff Adinolfi otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

126. Plaintiff Adinolfi further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

127. The Data Breach has caused Plaintiff Adinolfi to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key

details about the Data Breach's occurrence.

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

129. As a result of the Data Breach, Plaintiff Adinolfi is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

130. Plaintiff Adinolfi has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

C. Plaintiff John Moss

131. Plaintiff Moss's information was stored with Defendant as a result of his dealings with Defendant.

132. Plaintiff Moss obtained life insurance through Prudential and utilized Prudential for its products and services related to investments. Plaintiff Moss also purchased life insurance policies for his daughter and his grandson and opened a Roth IRA account for his daughter through Prudential. Plaintiff Moss closed the accounts for his daughter and grandson about 10 years ago. To use Defendant's services and products, Plaintiff Moss—like other Class Members—provided sensitive Private Information including his full name, address, date of birth, and insurance information.

133. Defendant obtained and continues to store and maintain Plaintiff's Private Information. Defendant owes Plaintiff Moss a legal duty and obligation to protect his Private Information from unauthorized access and disclosure. Prudential notified Plaintiff Moss on June 24, 2024, nearly five months after it had discovered the Data Breach, that Plaintiff Moss's Private

Information was compromised in the Data Breach and disclosed as a result of Defendant's inadequate data security practices.

134. Over eight months after the Data Breach, Defendant has yet to confirm the exact information that was compromised in the Data Breach. However, on information and belief, Class Members' compromised data includes, but is not limited to: customer first name, last name, address, date of birth, policy numbers, addresses, email addresses, phone numbers, Social Security numbers, credit card information, debit card information, financial account information, driver's license information, health treatment information, health diagnosis information, prescription information, and health condition information.

135. Plaintiff Moss is very careful with his Private Information. He stores any documents containing his Private Information in a safe and secure location or destroys the documents. Plaintiff Moss has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Moss diligently chooses unique usernames and passwords for his various online accounts.

136. As a result of the Data Breach, Plaintiff Moss made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring his credit.

137. Plaintiff Moss was forced to spend multiple hours attempting to mitigate the effects of the Data Breach. He will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to time with his family, work and/or recreation. This is time that is lost forever and cannot be recaptured.

138. Plaintiff Moss suffered actual injury and damages as a result of the Data Breach

including, but not limited to: (a) damage to and diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Moss; (b) violation of his privacy rights; (c) the theft of his Private Information; (d) loss of time; (e) imminent and impending injury arising from the increased risk of identity theft and fraud; (f) increased out-of-pocket medical expenses; (g) failure to receive the benefit of his bargain; and (h) nominal and statutory damages.

139. Plaintiff Moss has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud.

140. As a result of the Data Breach, Plaintiff Moss anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Moss will continue to be at a present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

141. Plaintiff Moss has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

D. Plaintiff Stepanie Demaro

142. Plaintiff Demaro's information was stored with Defendant as a result of her dealings with Defendant.

143. Plaintiff Demaro utilized Prudential's services and products for her retirement, children's college, and life insurance investments. While Plaintiff Demaro no longer utilizes

Prudential for her retirement investments, for almost 20 years, she has and continues to use Prudential for her children's college investments and life insurance. To use Defendant's services, Plaintiff Demaro—like other Class Members—provided sensitive Private Information, including her full name, address, date of birth, phone number, and more.

144. Defendant obtained, stored and maintained Plaintiff Demaro's and Class Members' Private Information. Defendant owes Plaintiff Demaro a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Prudential notified Plaintiff Demaro on June 10, 2024, over four months after it had discovered the Data Breach, that her Private Information was compromised in the Data Breach and disclosed as a result of Defendant's inadequate data security practices.

145. Over eight months after the Data Breach, Defendant has yet to confirm the exact information that was compromised in the Data Breach. However, on information and belief, Class Members' compromised data includes, but is not limited to: customer first name, last name, address, date of birth, policy numbers, addresses, email addresses, phone numbers, Social Security numbers, credit card information, debit card information, financial account information, driver's license information, health treatment information, health diagnosis information, prescription information, and health condition information.

146. Plaintiff Demaro is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff Demaro has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Demaro diligently chooses unique usernames and passwords for her various online accounts.

147. As a result of the Data Breach, Plaintiff Demaro made reasonable efforts to mitigate

the impact of the Data Breach after receiving the Data Breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit.

148. Plaintiff Demaro has been forced to spend multiple hours attempting to mitigate the effects of the Data Breach. She will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to time with her family, work and/or recreation. This is time that is lost forever and cannot be recaptured.

149. Plaintiff Demaro suffered actual injury and damages as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of her Private Information, a form of intangible property that Defendant obtained from Plaintiff Demaro; (b) violation of her privacy rights; (c) the theft of her Private Information; (d) loss of time; (e) imminent and impending injury arising from the increased risk of identity theft and fraud; (f) increased out-of-pocket medical expenses; (g) failure to receive the benefit of her bargain; and (h) nominal and statutory damages.

150. Plaintiff Demaro has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud.

151. As a result of the Data Breach, Plaintiff Demaro anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Demaro will continue to be at a present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

152. Plaintiff Demaro has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

E. Plaintiff Anthony Guissarri

153. Plaintiff Guissarri's information was stored with Defendant as a result of his dealings with Defendant.

154. Plaintiff Guissarri has utilized Prudential's services and products for financial investments and retirement since 1985. To use Defendant's services, Plaintiff Guissari—like other Class Members—provided sensitive Private Information including his full name, address, date of birth, phone number, Social Security number and more.

155. Defendant obtained, stored and maintained Plaintiff Guissarri's and Class Members' Private Information. Defendant owes Plaintiff Guissarri a legal duty and obligation to protect his Private Information from unauthorized access and disclosure.

156. Prudential notified Plaintiff Guissarri on June 10, 2024, over four months after it had discovered the Data Breach, that his Private Information was compromised in the Data Breach and disclosed as a result of Defendant's inadequate data security practices.

157. Over eight months after the Data Breach, Defendant has yet to confirm the exact information that was compromised in the Data Breach. However, on information and belief, Class Members' compromised data includes, but is not limited to: customer first name, last name, address, date of birth, policy numbers, addresses, email addresses, phone numbers, Social Security numbers, credit card information, debit card information, financial account information, driver's license information, health treatment information, health diagnosis information, prescription information, and health condition information.

158. Plaintiff Guissarri is very careful with his Private Information. He stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff Guissarri has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Guissarri diligently chooses unique usernames and passwords for his various online accounts.

159. As a result of the Data Breach, Plaintiff Guissarri made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring his credit.

160. Despite his best efforts, Plaintiff Guissarri became aware that someone attempted to file a fraudulent 2023 IRS Tax Return using his Private Information.

161. Plaintiff Guissarri has been forced to spend multiple hours attempting to mitigate the effects of the Data Breach. He will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to time with his family, work and/or recreation. This is time that is lost forever and cannot be recaptured.

162. Plaintiff Guissarri suffered actual injury and damages as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Guissarri; (b) violation of his privacy rights; (c) the theft of his Private Information; (d) loss of time; (e) past, imminent and impending injury arising from the increased risk of identity theft and fraud; (f) increased out-of-pocket medical expenses; (g) failure to receive the benefit of his bargain; and (h) nominal and statutory damages.

163. Plaintiff Guissarri has also suffered emotional distress that is proportional to the

risk of harm and loss of privacy caused by the theft of her Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud.

164. As a result of the Data Breach, Plaintiff Guissarri anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Guissarri will continue to be at a present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

165. Plaintiff Guissarri has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

F. Plaintiff Roger Menhennett

166. Plaintiff Menhennett's information was stored with Defendant as a result of his dealings with Defendant.

167. Plaintiff Menhennett utilized Prudential's services and products for financial investments and retirement. To use Defendant's services, Plaintiff Menhennett—like other Class Members—provided sensitive Private Information including his full name, address, date of birth, phone number, Social Security number and more.

168. Defendant obtained, stored and maintained Plaintiff Menhennett's and Class Members' Private Information. Defendant owes Plaintiff Menhennett a legal duty and obligation to protect his Private Information from unauthorized access and disclosure.

169. Prudential notified Plaintiff Menhennett on June 13, 2024, over four months after it had discovered the Data Breach, that his Private Information was compromised in the Data

Breach and disclosed as a result of Defendant's inadequate data security practices.

170. Over eight months after the Data Breach, Defendant has yet to confirm the exact information that was compromised in the Data Breach. However, on information and belief, Class Members' compromised data includes, but is not limited to: customer first name, last name, address, date of birth, policy numbers, addresses, email addresses, phone numbers, Social Security numbers, credit card information, debit card information, financial account information, driver's license information, health treatment information, health diagnosis information, prescription information, and health condition information.

171. Plaintiff Menhennett is very careful with his Private Information. He stores any documents containing his Private Information in a safe and secure location or destroys the documents. Plaintiff Menhennett has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Menhennett diligently chooses unique usernames and passwords for his various online accounts.

172. As a result of the Data Breach, Plaintiff Menhennett made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring his credit.

173. Plaintiff Menhennett has been forced to spend multiple hours attempting to mitigate the effects of the Data Breach. He will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to time with his family, work and/or recreation. This is time that is lost forever and cannot be recaptured.

174. Plaintiff Menhennett suffered actual injury and damages as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his Private

Information, a form of intangible property that Defendant obtained from Plaintiff Menhennett; (b) violation of his privacy rights; (c) the theft of his Private Information; (d) loss of time; (e) imminent and impending injury arising from the increased risk of identity theft and fraud; (f) increased out-of-pocket medical expenses; (g) failure to receive the benefit of his bargain; and (h) nominal and statutory damages.

175. Plaintiff Menhennett has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of her Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud.

176. As a result of the Data Breach, Plaintiff Menhennett anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Menhennett will continue to be at a present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

177. Plaintiff Menhennett has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

VI. CLASS ACTION ALLEGATIONS

178. Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure ("F.R.C.P.") on behalf of Plaintiffs and the following classes/subclass(es) (collectively, the "Class(es)"):

> "All individuals within the United States of America whose Private Information was compromised in the Data Breach." ("**Nationwide Class**")[31].

[31] Unless stated otherwise, all references to the "Class" shall refer to the Nationwide Class.

Additionally Plaintiff Anthony Guissarri seeks to represent the following California Subclass:

> "All individuals within the State of California whose Private Information was compromised in the Data Breach." ("**California Subclass**").

Additionally, Plaintiff Gina Adinolfi seeks to represent the following New Jersey Subclass:

> "All individuals within the State of New Jersey whose Private Information was compromised in the Data Breach." ("**New Jersey Subclass**").

Additionally, Plaintiff Roger Menhennett seeks to represent the following New York Subclass:

> "All individuals within the State of New York whose Private Information was compromised in the Data Breach." ("**New York Subclass**").

179. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

180. Plaintiffs reserve the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

181. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

182. Numerosity: A class action is the only available method for the fair and efficient

adjudication of this controversy, as the members of the Class and each State Subclass are so numerous that joinder of all members is impractical, if not impossible. As of June 28, 2024, Defendant has identified 2,556,210 individuals affected by the Data Breach. Prudential discovery will ultimately identify the customers whose Private Information was improperly accessed in the Data Breach. Those individuals' names and addresses are available from Prudential's records, and Class and Subclass Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of Class Members in each Subclass, making joinder of all Subclass Members impracticable.

183. Commonality: Plaintiffs and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law that predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendant had a legal duty to Plaintiffs, the Class, and Subclasses to exercise due care in collecting, storing, maintaining, using, and/or safeguarding their Private Information;

b. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

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

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

e. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

f. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

g. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class and Subclass Members that their Private Information had been compromised;

h. How and when Defendant actually learned of the Data Breach;

i. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Private Information of Plaintiffs and Class and Subclass Members;

j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

k. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class and Subclass Members;

l. Whether Defendant violated the state consumer protection statutes invoked below;

m. Whether Plaintiffs and Class and Subclass Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct; and

n. Whether Plaintiffs and Class and Subclass Members are entitled to restitution as a result of Defendant's wrongful conduct.

184. Typicality: Plaintiffs' claims are typical of the claims of the Class and their respective Subclasses. Plaintiffs and all members of the Class and Subclasses sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

185. Adequacy of Representation: Plaintiffs in this class action are an adequate representative of the Class and their respective Subclasses in that Plaintiffs have the same interest in the litigation of this case as Class and Subclass Members, are committed to the vigorous prosecution of this case, and have retained competent counsel who are experienced in conducting litigation of this nature.

186. Predominance: Defendant has engaged in a common course of conduct towards Plaintiffs and Class and Subclass Members, in that all the data of Plaintiffs and Class and Subclass Members was stored on the same network and unlawfully accessed in the same way. The common

issues arising from Defendant's conduct affecting Class and Subclass 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.

187. Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class and Subclass Members or the classes in their entirety. Plaintiffs anticipate no management difficulties in this litigation.

188. Superiority of Class Action: Since the damages suffered by individual Class and Subclass Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Class and Subclasses to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or required to be brought by each member of the Class or Subclasses, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

189. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class and Subclass Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

190. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class and Subclass Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class and Subclass Members and making final injunctive relief appropriate with respect to the Classes in their entirety.

191. Defendant's policies and practices challenged herein apply to and affect Class and

Subclass Members uniformly, and Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Classes in their entirety, not on facts or law applicable only to Plaintiffs.

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

a. Whether Defendant failed to notify the public of the Data Breach timely;

b. Whether Defendant owed a legal duty to Plaintiffs, the Class, and the Subclasses to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures and workforce training protocols to protect their data systems were reasonable and adequate in light of best practices recommended by data security experts;

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

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

193. Unless a classwide injunction is issued, Defendant may continue failing to secure the Private Information of Class and Subclass Members properly, and Defendant may continue to act unlawfully as set forth in this Complaint.

194. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and Subclasses and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class and Subclass Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

195. Plaintiffs reallege and reincorporate every factual allegation set forth in the preceding paragraphs as though fully set forth herein.

196. By collecting and storing the Private Information of Plaintiffs and Class Members, in their computer systems and networks, and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

197. At all times herein relevant, Defendant owed Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their Private Information and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the Private Information of Plaintiffs and Class Members in its computer systems and on its networks.

198. Among these duties, Defendant was expected:

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

b. to protect Plaintiffs' and Class Members' Private Information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiffs and Class Members of any data breach,

security incident, or intrusion that affected or may have affected their Private Information.

199. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

200. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information, the vulnerabilities of its data security systems, and the importance of adequate security.

201. Defendant knew about numerous, well-publicized data breaches.

202. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs' and Class Members' Private Information.

203. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the Private Information that Plaintiffs and Class Members had entrusted to it.

204. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their Private Information.

205. Because Defendant knew that a breach of its systems could damage millions of individuals, including Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the Private Information contained therein.

206. Plaintiffs' and Class Members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant would take adequate security precautions.

207. Moreover, only Defendant had the ability to protect its systems and the Private

Information stored on them from attack. Thus, Defendant had a special relationship with Plaintiffs and Class Members.

208. Defendant's duties also arose under HIPPA regulations, which, as described above, applied to Defendant and establish national standards for the protection of patient information, including protected health information, which required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

209. Defendant's duties also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits their "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 personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

210. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiffs, and/or the remaining Class Members.

211. Defendant breached its general duty of care to Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members;

b. by failing to timely and accurately disclose that Plaintiffs' and Class Members' Private Information had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the Private Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information;

d. by failing to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Private Information of Plaintiffs and Class Members, misuse the Private Information and intentionally disclose it to others without consent.

e. by failing to adequately train its employees not to store Private Information longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiffs' and Class Members' Private Information;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. by failing to encrypt Plaintiffs' and Class Members' Private Information and monitor user behavior and activity in order to identify possible threats.

212. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

213. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages.

214. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Private Information to Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their Private Information.

215. Defendant breached its duty to notify Plaintiffs and Class Members of the

unauthorized access by waiting months after learning of the Data Breach to notify Plaintiffs and Class Members and then by failing and continuing to fail to provide Plaintiffs and Class Members sufficient information regarding the breach.

216. To date, Defendant has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and Class Members.

217. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their Private Information.

218. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiffs and Class Members.

219. Plaintiffs' and Class Members' Private Information was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

220. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

221. The damages Plaintiffs and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

222. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to decide how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with

the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) 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 embarrassment and identity theft; (vi) the continued risk to their Private Information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information in its continued possession; and (vii) 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.

223. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

224. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

COUNT TWO
Negligence *Per Se*
(On behalf of Plaintiffs and the Nationwide Class)

225. Plaintiffs reallege and reincorporate every factual allegation set forth in the

preceding paragraphs as though fully set forth herein.

226. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits companies such as Defendant from "using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce," including failing to use reasonable measures to protect Private Information. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

227. In addition to the FTC rules and regulations and state law, other states and jurisdictions where victims of the Data Breach are located require that Defendant protect Private Information from unauthorized access and disclosure and timely notify the victim of a data breach.

228. Defendant violated FTC rules and regulations obligating companies to use reasonable measures to protect Private Information by failing to comply with applicable industry standards and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a Data Breach and the exposure of Representative Plaintiff's and Class members' highly sensitive Private Information.

229. Each of Defendant's statutory violations of Section 5 of the FTC Act and other applicable statutes, rules and regulations, constitute negligence per se.

230. Plaintiffs and Class Members are within the category of persons the FTC Act were intended to protect.

231. The harm that occurred because of the Data Breach described herein is the type of harm the FTC Act was intended to guard against.

232. In addition, Defendant is an entity covered by HIPAA (45 C.F.R. § 160.102) and

as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

233. HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

234. HIPAA further requires Defendants to disclose the unauthorized access and theft of the Personal Information to Plaintiffs and the Class Members "without unreasonable delay" so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. See 45 C.F.R. §§ 164.404, 406, 410.

235. Defendants violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' Personal Information, as described herein.

236. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class Members have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their Private Information in Defendant's possession and are entitled to damages in an amount to be proven at trial.

COUNT THREE
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class)

237. Plaintiffs reallege and reincorporate every factual allegation set forth in the preceding paragraphs as though fully set forth herein.

238. Through its course of conduct, Defendant, Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

239. Defendant required Plaintiffs and Class Members to provide and entrust their Private Information as a condition of obtaining Defendant's services.

240. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices.

241. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

242. As a condition of their relationship with Defendant, Plaintiffs and Class Members provided and entrusted their Private Information to Defendant.

243. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

244. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their Private Information to Defendant, in exchange for, amongst other things, the protection of their Private Information.

245. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

246. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data

Breach.

247. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

COUNT FOUR
Breach of Confidence
(On behalf of Plaintiffs and the Nationwide Class)

248. Plaintiffs reallege and reincorporate every factual allegation set forth in the preceding paragraphs as though fully set forth herein.

249. During Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential nature of the Private Information that Representative Plaintiffs and Class Members provided to it.

250. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by promises and expectations that Plaintiffs' and Class Members' Private Information would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

251. Plaintiffs and Class Members provided their respective Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be accessed by, acquired by, appropriated by, disclosed to,

encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

252. Plaintiffs and Class Members also provided their Private Information to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their Private Information from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting its networks and data systems.

253. Defendant voluntarily received, in confidence, Plaintiffs' and Class Members' Private Information with the understanding that the Private Information would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

254. Due to Defendant's failure to prevent, detect and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiffs' and Class Members' confidence and without their express permission.

255. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages, as alleged herein.

256. But for Defendant's failure to maintain and protect Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third

parties. The Data Breach was the direct and legal cause of the misuse of Plaintiffs' and Class Members' Private Information and the resulting damages.

257. The injury and harm Plaintiffs and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiffs' and Class Members' Private Information. Defendant knew its data systems and protocols for accepting and securing Plaintiffs' and Class Members' Private Information had security and other vulnerabilities that placed Plaintiffs' and Class Members' Private Information in jeopardy.

258. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' Private Information in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, (vii) the diminished value of Plaintiffs' and Class Members' Private Information, and (viii) the diminished value of Defendant's services for which Plaintiffs and Class Members paid and received.

COUNT FIVE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiffs and the Nationwide Class)

259. Plaintiffs reallege and reincorporate every factual allegation set forth in the preceding paragraphs as though fully set forth herein.

260. Every contract in this state has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

261. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

262. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

263. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT SIX
Unjust Enrichment
(On behalf of Plaintiffs and the Nationwide Class)

264. Plaintiffs reallege and reincorporate every factual allegation set forth in the preceding paragraphs as though fully set forth herein.

265. By its wrongful acts and omissions described herein, Defendant has obtained a

benefit by unduly taking advantage of Plaintiffs and Class Members.

266. Defendant, prior to and at the time Plaintiffs and Class Members entrusted their Private Information to Defendant, caused Plaintiffs and Class Members to reasonably believe that Defendant would keep such Private Information secure.

267. Defendant was aware, or should have been aware, that reasonable patients and consumers would have wanted their Private Information kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

268. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiffs' and Class Members' decisions to seek services therefrom.

269. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiffs and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

270. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiffs and Class Members the ability to make a rational and informed purchasing and servicing decision and took undue advantage of Plaintiffs and Class Members.

271. Defendant was unjustly enriched at the expense of Plaintiffs and Class Members, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiffs and Class Members; however, Plaintiffs and Class Members did not receive the benefit of their bargain because they paid for products and or services that did not satisfy the purposes for which they bought/sought them.

272. Since Defendant's profits, benefits, and other compensation were obtained improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

273. Plaintiffs and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiffs and Class Members may seek restitution.

COUNT SEVEN
Bailment
(On behalf of Plaintiffs and the Nationwide Class)

274. Plaintiffs reallege and reincorporate by reference all factual allegations above as if fully set forth herein.

275. Plaintiffs and Class Members provided Private Information to Defendant, which Defendant was under a duty to keep private and confidential.

276. Plaintiffs' and Class Members' Private Information is personal property and was conveyed to Defendant for the certain purpose of keeping the information private and confidential.

277. Plaintiffs' and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendant was aware of the risks it took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

278. Once Defendant accepted Plaintiffs' and Class Members' Private Information, it was in the exclusive possession of that information, and neither Plaintiffs nor Class Members could control that information once it was within the possession, custody, and control of Defendant.

279. Defendant did not safeguard Plaintiffs' or Class Members' Private Information when it failed to adopt and implement reasonable and adequate data security safeguards to prevent the known risk of a cyberattack.

280. Defendant's failure to safeguard Plaintiffs' and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

281. As a result of Defendant's failure to keep Plaintiffs' and Class Members' Private Information secure, Plaintiffs and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

COUNT EIGHT
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Nationwide Class)

282. Plaintiffs reallege and reincorporate by reference all factual allegations above as if fully set forth herein.

283. In light of the special relationship between Defendant and Plaintiffs and Class Members, Defendant became fiduciaries by undertaking a guardianship of the Private Information to act primarily for Plaintiffs and Class Members: (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant do store.

284. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship to keep secure their Private Information.

285. Defendant breached their fiduciary duty to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

286. Defendant breached their fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

287. As a direct and proximate result of Defendant's breach of their fiduciary duties,

Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

288. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT NINE
Declaratory Judgment
(On behalf of Plaintiffs and the Nationwide Class)

289. Plaintiffs reallege and reincorporate by reference all factual allegations above as if fully set forth herein.

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

291. An actual controversy has arisen after the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs continue to suffer injury due to the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

292. Plaintiffs and the Classes have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including: (i) Defendant's failure to encrypt Plaintiffs' and Class Members' Private Information, including Social Security numbers, while storing it in an Internet-accessible environment, and (ii) Defendant's failure to delete Private Information it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Plaintiffs.

293. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the Private Information of Plaintiffs and Class Members;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information;

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs harm.

294. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law, industry, and government regulatory standards to protect consumers' Private Information. Specifically, this injunction

should, among other things, direct Defendant to:

a. engage third-party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards; and

d. implement an education and training program for appropriate employees regarding cybersecurity.

295. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

296. The hardship to Plaintiffs, if an injunction is not issued, exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to use such measures.

297. Issuance of the requested injunction will satisfy the public interest. Such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

COUNT TEN
Violations of New York General Business Law
N.Y. Gen. Bus. Law § 349, *et seq.*
(On Behalf of Plaintiff Menhennett and New York Subclass)

298. Plaintiff Menhennett ("Plaintiff" for purposes of this Count), individually and on behalf of the New York Subclass, repeats the factual allegations contained in the preceding paragraphs as if fully set forth herein.

299. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New York Subclass Members' Personal Information, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and New York Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and New York Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not

> comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

300. Plaintiff and members of the New York Subclass were deceived in New York. They also transacted with Defendant in New York by utilizing Defendant's services in New York.

301. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

302. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff's and New York Subclass Members' rights. Prudential's past data breach and breaches within the health industry put them on notice that its security and privacy protections were inadequate.

303. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

304. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including New Yorkers affected by the Data Breach.

305. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably

avoid.

306. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

COUNT ELEVEN
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.100, *et seq*.
(On Behalf of Plaintiff Guissarri and California Subclass)

307. Plaintiff Guissarri ("Plaintiff" for purposes of this Count), individually and on behalf of the California Subclass, repeats the factual allegations contained in the preceding paragraphs as if fully set forth herein.

308. At all relevant times, Defendant was a "business" under the terms of the CCPA as a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity operating in the State of California that collects consumers' personal information, and that have annual operating revenue above $25 million.

309. At all relevant times, Plaintiff and the California Subclass Members were "consumers" under the terms of the CCPA as natural persons as defined in Section 17014 of Title 18 of the California Code of Regulations.

310. By the acts described above, Defendant violated the CCPA by negligently and recklessly collecting, maintaining, and controlling its customers' sensitive personal medical information and by designing, maintaining, and controlling systems that exposed its customers' sensitive personal medical information of which Defendant had control and possession to the risk of exposure to unauthorized persons, thereby violating their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. Defendant allowed unauthorized users to view, use, manipulate,

exfiltrate, and steal the nonencrypted and nonredacted personal information of Plaintiff and other customers, including their personal medical information.

311. Plaintiff has complied with the requirements of California Civil Code section 1798.150(b) providing Defendant with written notice of the specific provisions of the CCPA Plaintiff alleges have been violated via certified mail per the law.

312. As a result of Defendant's violations, Plaintiff and the California Subclass are entitled to all actual and compensatory damages according to proof or statutory damages allowable under the CCPA, whichever are higher, and to such other and further relief as this Court may deem just and proper.

COUNT TWELVE
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff Guissarri and the California Subclass)

313. Plaintiff Guissarri ("Plaintiff" for purposes of this Count), individually and on behalf of the California Subclass, repeats the factual allegations contained in the preceding paragraphs as if fully set forth herein.

314. To assert claims for intrusion upon seclusion, one must plead (1) that the defendant intentionally intruded into a matter as to which Plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

315. Defendant intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff and California Subclass Members by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiff's and California Subclass Members' personal information. Only Defendant had control over its systems.

316. Defendant's conduct is especially egregious and offensive as it failed to have adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiff's and California Subclass Members' personal information.

317. At all times, Defendant was aware that Plaintiff's and California Subclass Members' Private Information in its possession contained highly sensitive and confidential personal information.

318. Plaintiff and California Subclass Members have a reasonable expectation of privacy in their personal information, which also contains highly sensitive medical information.

319. Defendant intentionally configured its systems in such a way that stored Plaintiff's and California Subclass Members' Private Information to be left vulnerable to malware/ransomware attacks without regard for Plaintiff's and California Subclass Members' privacy interests.

320. The disclosure of thousands of consumers' sensitive and confidential personal information was highly offensive to Plaintiff and California Subclass Members because it violated expectations of privacy that have been established by general social norms, including by granting access to private information and data that would not otherwise be disclosed.

321. Defendant's conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. Defendant's conduct would be especially egregious to a reasonable person as Defendant publicly disclosed Plaintiff's and California Subclass Members' sensitive and confidential personal information without their consent to an "unauthorized person," i.e., hackers.

322. As a result of Defendant's actions, Plaintiff and California Subclass Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

323. Plaintiff and California Subclass Members have been damaged as a direct and proximate result of Defendant's intrusion upon seclusion and are entitled to just compensation.

324. Plaintiff and California Subclass Members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened stress, fear, anxiety and risk of future invasions of privacy.

COUNT THIRTEEN
Invasion of Privacy – Cal. Const. Art. 1, § 1
(On Behalf of Plaintiff Guissarri and the California Subclass)

325. Plaintiff Guissarri ("Plaintiff" for purposes of this Count), individually and on behalf of the California Subclass, repeats the factual allegations contained in the preceding paragraphs as if fully set forth herein.

326. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

327. The right to privacy in California's constitution creates a private right of action against private and government entities.

328. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

329. Defendant violated Plaintiff's and California Subclass Members' constitutional right to privacy by collecting, storing, and disclosing their personal information in which they had a legally protected privacy interest, and in which they had a reasonable expectation of privacy in,

in a manner that was highly offensive to Plaintiff and California Subclass Members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

330. Defendant has intruded upon Plaintiff's and California Subclass Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

331. Defendant's actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the invasion occurred within a zone of privacy protected by the California Constitution, namely the misuse of information gathered for an improper purpose; and (ii) the invasion deprived Plaintiff and California Subclass Members of the ability to control the circulation of their personal information, which is considered fundamental to the right to privacy.

332. Plaintiff and California Subclass Members had a reasonable expectation of privacy in that: (i) Defendant's invasion of privacy occurred as a result of Defendant's security practices including the collecting, storage, and unauthorized disclosure of consumers' personal information; (ii) Plaintiff and California Subclass Members did not consent or otherwise authorize Defendant to disclosure their personal information; and (iii) Plaintiff and California Subclass Members could not reasonably expect Defendant would commit acts in violation of laws protecting privacy.

333. As a result of Defendant's actions, Plaintiff and California Subclass Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation.

334. Plaintiff and California Subclass Members suffered actual and concrete injury as a result of Defendant's violations of their privacy interests. Plaintiff and California Subclass Members are entitled to appropriate relief, including damages to compensate them for the harm to

their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

335. Plaintiff and California Subclass Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and California Subclass Members for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and California Subclass Members' privacy.

COUNT FOURTEEN
Violation of Cal. Civ. Code § 1798.81.5
(On Behalf of Plaintiff Guissarri and the California Subclass)

336. Plaintiff Guissarri ("Plaintiff" for purposes of this Count), individually and on behalf of the California Subclass, repeats the factual allegations contained in the preceding paragraphs as if fully set forth herein.

337. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

338. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

339. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

340. Plaintiff and California Subclass Members are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant, directly and/or indirectly, for the purpose of obtaining a service from Defendant.

341. The personal information of Plaintiff and the California Subclass Members constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; and (v) health insurance information.

342. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass's personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the California Subclass from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected

Plaintiff's and the California Subclass's nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

343. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the California Subclass Members included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the California Subclass Members by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

344. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the California Subclass were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the Subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff and the California Subclass seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

345. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

346. Any person or business that is required to issue a security breach notification must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

1) the date of the breach,

2) the estimated date of the breach, or

3) the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

347. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California Subclass. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all Subclass

Members. Because not all Subclass Members have been notified of the breach, Subclass Members could have taken action to protect their personal information, but were unable to do so because they were not timely notified of the breach.

348. On information and belief, many Subclass Members affected by the Data Breach have not received any notice at all from Defendant in violation of Section 1798.82(d).

349. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and California Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

350. As a direct consequence of the actions as identified above, Plaintiff and California Subclass Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the Data Breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

COUNT FIFTEEN
Violation of Cal. Bus. & Prof. Code § 17200
(On Behalf of Plaintiff Guissarri and California Subclass)

351. Plaintiff Guissarri ("Plaintiff" for purposes of this Count), individually and on behalf of the California Subclass, repeats the factual allegations contained in the preceding paragraphs as if fully set forth herein.

352. Plaintiff and California Subclass Members further bring this cause of action,

seeking equitable and statutory relief to stop the misconduct of Defendant, as complained of herein.

353. Defendant has engaged in unfair competition within the meaning of California Business & Professions Code §§ 17200, *et seq.*, because its conduct was/is unlawful, unfair, and/or fraudulent, as herein alleged.

354. Plaintiff and the California Subclass Members, and Defendant are each a "person" or "persons" within the meaning of § 17201 of the California Unfair Competition Law ("UCL").

355. The knowing conduct of Defendant, as alleged herein, constitutes an unlawful and/or fraudulent business practice, as set forth in California Business & Professions Code §§ 17200-17208. Specifically, Defendant conducted business activities while failing to comply with the legal mandates cited herein. Such violations include, but are not necessarily limited to:

a. failure to maintain adequate computer systems and data security practices to safeguard PII;

b. failure to disclose that their computer systems and data security practices were inadequate to safeguard PHI/PII from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiff and California Subclass Members;

d. continued acceptance of PHI/PII and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of PHI/PII and storage of other personal information after Defendants knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

356. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiff and California Subclass Members, deter hackers, and detect a breach within a reasonable time and that the risk of a data breach was highly likely.

357. In engaging in these unlawful business practices, Defendant has enjoyed an advantage over its competition and a resultant disadvantage to the public and California Subclass Members.

358. Defendant's knowing failure to adopt policies in accordance with and/or adhere to these laws, all of which are binding upon and burdensome to Defendant's competitors, engenders an unfair competitive advantage for Defendant, thereby constituting an unfair business practice, as set forth in California Business & Professions Code §§ 17200-17208.

359. Defendant has clearly established a policy of accepting a certain amount of collateral damage, as represented by the damages to Plaintiff and California Subclass Members herein alleged, as incidental to their business operations, rather than accept the alternative costs of full compliance with fair, lawful, and honest business practices ordinarily borne by responsible competitors of Defendant and as set forth in legislation and the judicial record.

360. The UCL is, by its express terms, a cumulative remedy, such that remedies under its provisions can be awarded in addition to those provided under separate statutory schemes and/or common law remedies, such as those alleged in the other causes of action in this Complaint. *See* Cal. Bus. & Prof. Code § 17205.

361. Plaintiff and California Subclass Members request that this Court enter such orders or judgments as may be necessary to enjoin Defendant from continuing its unfair, unlawful, and/or deceptive practices and to restore to Plaintiff and California Subclass Members any money Defendant acquired by unfair competition, including restitution and/or equitable relief, including disgorgement of ill-gotten gains, refunds of moneys, interest, reasonable attorneys' fees, and the costs of prosecuting this class action, as well as any and all other relief that may be available at law or equity.

COUNT SIXTEEN
Violation of the New Jersey Consumer Fraud Act, N.J. S.A. §§ 56:8-1, *et seq.*
(On Behalf of Plaintiff Gina Adinolfi and the National Class
or, in the alternative, the New Jersey Subclass)

362. Plaintiff Adinolfi ("Plaintiff" for purposes of this Count), individually and on behalf of the National Class or, in the alternative, the New Jersey Subclass, repeats and re-alleges the factual allegations contained in the preceding paragraphs as if fully set forth herein.

363. Prudential is a "person," as defined by N.J.S.A. § 56:8-1(d).

364. Prudential sells "merchandise," as defined by N.J.S.A. § 56:8-1(c) & (e).

365. The New Jersey Consumer Fraud Act ("CFA"), N.J.S.A. §§ 56:8-2, *et seq.* prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

366. New Jersey CFA claims for unconscionable commercial practice need not allege any fraudulent statement, representation, or omission by the defendant. *See Dewey v. Volkswagen AG*, 558 F. Supp. 2d 505, 525 (D.N.J. 2008); *see also Cox v. Sears Roebuck & Co.*, 138 N.J. 2, 19 (1994).

367. "The standard of conduct that the term 'unconscionable' implies is lack of 'good faith, honesty in fact and observance of fair dealing.'" *Cox*, 138 N.J. 2 at 18 (quoting *Kugler v. Romain*, 58 N.J. 522, 544 (1971)). "In addition, '[i]ntent is not an essential element' for allegations related to unconscionable commercial practices to succeed." *Fenwick v. Kay Am. Jeep, Inc.*, 72 N.J. 372, 379 (1977).

368. Prudential's handling and treatment of Plaintiff's, the Class Members', and the New Jersey Subclass Members' PII was unconscionable because:

a. Plaintiff, Class Members, and New Jersey Subclass Members had no choice but to provide their PII to Prudential to use their Prudential services.

b. To the extent that written contracts exist between Plaintiff, Class Members, and New Jersey Subclass Members on the one hand and Prudential on the other hand, those written contracts were made by Prudential and were not negotiable.

c. Once Plaintiff, Class Members, and Subclass Members provided their Private Information to Prudential protection of that Private Information was solely in Prudential's control. There is no way for Plaintiff, Class Members, and New Jersey Subclass Members to take any reasonable steps on their own to protect the Private Information in Prudential's hands, nor is there any way that Plaintiff, Class Members, and New Jersey Subclass Members would have any knowledge that it would be necessary for them to take steps on their own to protect their PII.

d. Prudential had a prior data security breach and, thus, knew or should have known that its data security was inadequate and needed to take additional security measures to protect Plaintiff, Class Members', and New Jersey Subclass Members' Private Information, but failed to do so, even though Prudential was the only entity in a position to protect Plaintiff, Class Members', and New Jersey Subclass Members' Private Information from wrongdoers.

e. Once Prudential became aware of the security breach, it failed to notify Plaintiff, Class Members, and Subclass Members of the Breach, thus depriving them of the opportunity to take measures to protect themselves from the effects of Prudential's failure to protect their Private Information.

f. Prudential's practices for handling and protecting Plaintiff, Class

Members', and New Jersey Subclass Members' Private Information was contrary to public policy in that Prudential failed to follow FTC and HIPAA guidelines with respect to the protection of Private Information and otherwise failed to follow industry standards for providing reasonable security and privacy measures to protect Plaintiff, Class Members', and New Jersey Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach.

369. Prudential's handling and treatment of Plaintiff's, the Class Members', and New Jersey Subclass Members' PII was deceptive because Prudential:

a. Misrepresented that it would protect the privacy and confidentiality of Plaintiff, Class Members', and New Jersey Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

b. Misrepresented that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff, Class Members', and New Jersey Subclass Members' Private Information, including duties imposed by FTC Act, 15 U.S.C. § 45, HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E, and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163, *et seq.*

c. Omitted, suppressed, and concealed the material fact that it did not properly secure Plaintiff, Class Members', and New Jersey Subclass Members' Private Information; and

d. Omitted, suppressed, and concealed the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff, Class Members', and New Jersey Subclass Members' Private Information, including duties

imposed by the FTC Act, 15 U.S.C. § 45, HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E, and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163, *et seq.*

370. Prudential's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Prudential's data security and ability to protect the confidentiality of consumers' PII.

371. Prudential intended to mislead Plaintiff, Class Members, and New Jersey Subclass Members and induce them to rely on its omissions of material fact.

372. Prudential acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff's, Class Members' and Subclass Members' rights. Prudential's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

373. As a direct and proximate result of Prudential's unconscionable and deceptive practices, Plaintiff, Class Members, and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Prudential's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

374. Plaintiff, Class Members, and New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual

damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and each member of the proposed Class(es), respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed class under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering them to cease from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs' and Class Members;

5. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an Order:

   a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

   c. requiring Defendant to delete and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when

weighed against the privacy interests of Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

f. prohibiting Defendant from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law;

and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

VIII. JURY DEMAND

Plaintiffs, individually and on behalf of the Class, hereby demand a trial by jury for all issues triable by jury.

Dated: October 17, 2024

Respectfully submitted,

By: */s/ Joseph J. DePalma*

Joseph J. DePalma
Catherine B. Derenze
LITE DEPALMA GREENBERG & AFANADOR, LLC
570 Broad Street, Suite 1201
Newark, NJ 07102
Tel: 973-623-3000
Fax: 973-623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

Andrew J. Sciolla (NJ bar 1889-2006)
SCIOLLA LAW FIRM LLC
Land Title Building
100 S. Broad Street, Suite 1910
Philadelphia, PA 19110
Tel: 267-328-5245
Fax: 215-972-1545
andrew@sciollalawfirm.com

Kevin Laukaitis (NJ bar 155722022)
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon, Suite 205, #10518
San Juan, PR 00907
Tel: (215) 789-4462
klaukaitis@laukaitislaw.com

James J. Pizzirusso*
HAUSFELD LLP
888 16th Street, N.W., Suite 300
Washington, D.C. 20006
Tel: (202) 540-7200
jpizzirusso@hausfeld.com

Steven M. Nathan*
HAUSFELD LLP
33 Whitehall Street, Fourteenth Floor
New York, NY 10004
Tel: (646) 357-1100
snathan@hausfeld.com

Daniel Srourian*
SROURIAN LAW FIRM
468 N. Camden Dr., Suite 200
Beverly Hills, CA 90210
Tel: (213) 474-3800
Fax: (213) 471-4160
daniel@slfla.com

Attorneys for Plaintiffs and the Putative Class

* *Admitted pro hac vice*