Adam T. Savett
WOLF POPPER LLP
570 Lexington Ave., 19th Floor
New York, NY 10023
Tel: (212) 759-4600
ASavett@wolfpopper.com

[Additional counsel listed on signature page]

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

MARIA D. CAPPUCCINO, as court-appointed guardian of ANGELO J. MONACO, an incapacitated person, and on behalf of all others similarly situated, Plaintiff, v. **BAYADA HOME HEALTH CARE, INC.,** Defendant.	Case No. 1:26-cv-10946 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Maria D. Cappuccino, as the court-appointed guardian of Angelo J. Monaco, an incapacitated person, brings this class action against Defendant Bayada Home Health Care, Inc. ("Bayada" or "Defendant") on behalf of Mr. Monaco and all others similarly situated. Plaintiff's allegations are based on personal knowledge as to herself and Mr. Monaco, and on information and belief, the investigation of counsel, and publicly available information as to all other matters.

INTRODUCTION

1. Bayada is one of the largest home health care providers in the country. Its patients are, by definition, people who need help. Many are elderly. Many are seriously ill. Many, like Angelo J. Monaco, have been adjudicated incapacitated and depend on a guardian to manage their affairs. These are the people who handed Bayada their most sensitive information — their diagnoses, their treatment histories, their Medicaid numbers, their dates of birth — because they had no realistic choice if they wanted care.

2. Bayada failed them. Between February 18, 2026 and March 2, 2026, an unauthorized person got into Bayada's computer network and copied files containing the private medical and personal information of Mr. Monaco and thousands of other people (the "Data Breach"). Bayada learned about the intrusion on March 2, 2026.

3. Bayada then said nothing for more than four months. It did not finish reviewing what had been taken until July 1, 2026. It did not mail notice letters until July 17, 2026 — **137 days after it discovered the breach** and **149 days after the intrusion began**. Federal law gave Bayada 60 days. Bayada took more than twice that long.

4. Every day Bayada stayed silent was a day Plaintiff could not protect Mr. Monaco, a day his information sat in a criminal's hands unmonitored, and a day the thief had a free head start.

5. The information Bayada lost about Mr. Monaco is exactly the kind that cannot be changed, cancelled, or reissued. According to Bayada's own notice letter, the files copied in the Data Breach contained Mr. Monaco's name, admission date, date of birth, diagnosis, diagnosis code, Medicaid identification, medical record number, payor authorization number, procedure type, subscriber member number, treating and referring physician, treatment cost information, and treatment location.

6. A person can get a new credit card. A person cannot get a new date of birth, a new medical history, or a new diagnosis. Once that information is out, it is out permanently, and it is worth far more to criminals than a credit card number. Stolen medical records sell on illegal marketplaces for multiples of what ordinary consumer data brings, precisely because they can be used to commit medical identity theft, bill fraudulent claims to Medicaid, obtain prescription drugs, and build convincing profiles for targeted fraud.

7. Bayada was not caught off guard by some unforeseeable event. Health care has been among the most heavily targeted industries in the country for years. Federal agencies have published repeated warnings about ransomware and data theft aimed at health care providers. Bayada knew or should have known that it was a target, and it knew the consequences of failure would fall on a uniquely vulnerable population.

8. Bayada also told its patients it was protecting them. Its published Privacy Notice for Clients states that it has "policies and procedures in place that protect your personal health information and restrict how it is used." Whatever those policies were, they did not stop an intruder from spending nearly two weeks inside Bayada's network and walking out with patient files.

9. Bayada's response has been as inadequate as its security. It offered affected people a single year of credit monitoring from **one** credit bureau. That offer is mismatched to the harm in at least three ways. First, the risk from stolen medical and Medicaid data does not expire in twelve months; it lasts for the rest of a person's life. Second, single-bureau monitoring leaves two of the three national credit files unwatched. Third, credit monitoring does not detect medical identity theft or fraudulent Medicaid billing at all — which is the most likely misuse of the specific data Bayada lost.

10. Bayada, not its patients, chose to collect this information. Bayada, not its patients, chose how to store it. Bayada, not its patients, chose to keep it long after treatment ended. Bayada, not its patients, chose to wait 137 days before saying anything. The costs of those choices should not fall on the patients.

11. Plaintiff, as guardian, brings this action on behalf of Mr. Monaco and on behalf of a nationwide Class of individuals whose private information was compromised in the Data Breach. She asserts claims on behalf of Mr. Monaco and

the Class for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, invasion of privacy, unjust enrichment, violation of the New Jersey Consumer Fraud Act, and declaratory judgment.

12. Plaintiff also brings claims on behalf of a Pennsylvania Subclass of members of the Class who are also Pennsylvania residents and asserts claims on behalf of Mr. Monaco and the Pennsylvania Subclass for violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law.

13. Plaintiff seeks money damages for the harm already done, and — just as importantly — an order requiring Bayada to fix the security failures that caused this breach and to provide monitoring that actually matches the lifetime risk it created.

PARTIES

A. Plaintiff

14. Angelo J. Monaco is a natural person and a citizen of the Commonwealth of Pennsylvania.

15. On April 14, 2014, upon a petition docketed as No. 651 of 2013, the Court of Common Pleas of Philadelphia County, Pennsylvania, Orphans' Court Division, adjudged Angelo J. Monaco to be an incapacitated person and appointed Angelo L. Monaco and Maria D. Cappuccino as plenary guardians of his person and of his estate. Those guardians have not been discharged and continue to serve.

16. Plaintiff Maria D. Cappuccino is a natural person and the duly appointed and acting guardian of Angelo J. Monaco. She brings this action solely in her capacity as guardian of Mr. Monaco, on his behalf and on behalf of the Class defined below. Her co-guardian, Angelo L. Monaco, has consented to the prosecution of these claims.

17. Mr. Monaco is an adjudicated incapacitated person who requires continuous, 24-hour assistance and support. He receives home- and community-based services through Pennsylvania's Consolidated Waiver pursuant to an Individual Support Plan ("ISP") that identifies and authorizes the services and supports necessary to address his needs. Bayada was a provider of services to Mr. Monaco under that arrangement and received Medicaid reimbursement for services furnished to him. In connection with those services, Bayada collected and stored his private personal and medical information, including the information identified in Bayada's July 17, 2026 notice letter.

18. Although Bayada was identified through Mr. Monaco's supports-coordination and ISP process, Ms. Cappuccino, acting as his guardian, retained the right to reject Bayada and obtain the authorized services from another qualified provider. Neither Ms. Cappuccino nor Mr. Monaco chose how Bayada would store his information, and they had no ability to negotiate over Bayada's data security. Ms. Cappuccino provided Mr. Monaco's information because Bayada required it as

a condition of receiving care, and Plaintiff reasonably relied on Bayada to keep it safe and to destroy it when it was no longer needed.

19. On or about July 17, 2026, Bayada mailed Mr. Monaco a letter at his home address notifying him that his private information had been compromised in the Data Breach. Mr. Monaco cannot independently evaluate the consequences of that disclosure, monitor his credit or Medicaid and insurance records for misuse, or enroll himself in the monitoring Bayada offered. Those protective responsibilities necessarily fall on Plaintiff and others acting on his behalf. As a result of the compromise of his Private Information, Mr. Monaco is a member of the Class.

B. Defendant

20. Defendant Bayada Home Health Care, Inc. is a corporation organized under the laws of the State of Delaware, with its headquarters and principal place of business at 4300 Haddonfield Road, Pennsauken, New Jersey 08109. Its registered agent is Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

21. Bayada provides home health care, hospice, pediatric home health, behavioral health, and personal care services to patients across the United States. It employs and has employed thousands of clinicians and staff. Its business depends on collecting, holding, and using patients' medical and personal information.

22. All of Bayada's decisions about how to secure patient information, how to investigate the Data Breach, and when and how to notify affected people were made or directed from its New Jersey headquarters.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action in which the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; there are more than 100 members of the proposed Class; and at least one member of the proposed Class is a citizen of a state different from Defendant. Mr. Monaco is a citizen of Pennsylvania, and Defendant is a citizen of Delaware and New Jersey.

24. The amount in controversy exceeds $5,000,000 based on, among other things, the number of people notified of the Data Breach, the nature and permanence of the information taken, the cost of the credit and medical identity monitoring necessary to address the risk Bayada created, the damages sustained by Mr. Monaco and Class Members, and the statutory and punitive damages sought.

25. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

26. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in this District, it is at home in this District, and it conducts substantial and continuous business in this District.

27. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) and (b)(2) because Defendant resides in this District and because a substantial part of the events giving rise to Plaintiff's claims — including Defendant's decisions about data security, its handling of the Data Breach, and its delayed notification — occurred in this District.

FACTUAL ALLEGATIONS

A. Bayada Collects Enormous Amounts of Deeply Private Information

28. Bayada delivers care in patients' homes. To do that, it collects and keeps a detailed picture of each patient's life and health.

29. As Bayada's own notice letter confirms, the information it maintained about Mr. Monaco included his name, admission date, date of birth, diagnosis, diagnosis code, Medicaid identification, medical record number, payor authorization number, procedure type, subscriber member number, treating and referring physician, treatment cost information, and treatment location.

30. Across the affected population, the categories of information Bayada has acknowledged were involved in the Data Breach include name, date of birth, diagnosis and medical or physical treatment information, provider information,

health insurance plan information, prescription information, hospital admission and discharge information, disability information, and Social Security numbers.

31. This information is referred to in this Complaint as "Private Information." It includes both personally identifiable information ("PII") and protected health information ("PHI") within the meaning of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations. See 45 C.F.R. § 160.103.

32. Bayada is a "covered entity" under HIPAA. 45 C.F.R. § 160.103.

33. Patients did not give Bayada this information as a favor or as a matter of choice. Bayada required it. A person who needs a home health aide, a nurse, or hospice care cannot decline to provide a diagnosis, a date of birth, or an insurance number and still get care.

34. Bayada also kept this information long after it was needed. On information and belief, Bayada retained the Private Information of former patients and former employees for years after their relationships with Bayada ended, without any legitimate business need to do so and without a reasonable data retention or destruction policy. Data that is deleted cannot be stolen. Every record Bayada kept past its useful life was an unnecessary risk that Bayada imposed on the person the record described.

B. Bayada Promised to Protect This Information

35. Bayada holds itself out to patients and their families as a trustworthy custodian of their health information.

36. Bayada's published Privacy Notice for Clients states that Bayada has "policies and procedures in place that protect your personal health information and restrict how it is used." *See* Bayada Home Health Care, Privacy Notice, https://www.bayada.com/privacy-notice.

37. Bayada made these representations to induce patients — including Mr. Monaco — to entrust it with their Private Information and to do business with it.

38. Bayada also had independent legal duties to protect this information, including under HIPAA's Security Rule and Privacy Rule, and under Section 5 of the Federal Trade Commission Act.

39. Implicit in every transaction between Bayada and its patients was a promise that Bayada would use reasonable measures to protect the Private Information it demanded, would notify patients promptly if that information was compromised, and would not keep the information longer than necessary.

40. Data security was a material part of what patients bargained for. Had Mr. Monaco and Class Members known that Bayada would fail to secure their information and would then sit on the news for more than four months, they would

not have entrusted their information to Bayada on the same terms, or would have insisted on different protections.

C. The Data Breach

41. On March 2, 2026, Bayada discovered that an unauthorized actor had gained access to its computer network.

42. Bayada's subsequent investigation determined that the unauthorized actor had access to Bayada's systems and **copied data from those systems between February 18, 2026 and March 2, 2026** — a period of approximately thirteen days.

43. In other words, an intruder was inside Bayada's network for nearly two weeks, moving through it and exfiltrating patient files, and Bayada did not notice. Bayada's own timeline is an admission that it lacked adequate monitoring, intrusion detection, and data loss prevention controls. A company with reasonable security does not let an outsider copy patient records for thirteen days undetected.

44. Bayada has never publicly explained how the intruder got in, what vulnerability was exploited, whether the attack involved ransomware, whether Bayada paid a ransom, how many people were affected in total, or what specific steps Bayada has taken since to prevent it from happening again. Bayada's notice letter is silent on all of these points. Plaintiff is left to guess about the scope of Mr. Monaco's exposure, and Class Members are left to guess about the scope of their own exposure.

45. Bayada reported the Data Breach to federal law enforcement and to the United States Department of Health and Human Services.

46. Bayada reported to the Texas Attorney General that at least 1,270 individuals were affected. *See* Texas Attorney General, Data Security Breach Reports, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage.

47. Bayada reported to the Vermont Attorney General that at least 6,097 **Vermont residents alone** were affected. *See* Vermont Attorney General, Security Breach Notices, https://ago.vermont.gov/categories/security-breach-notices.

48. Vermont is one of the least populous states in the country, and Bayada's national footprint dwarfs its Vermont operations. That more than six thousand Vermonters were notified strongly indicates that the nationwide affected population numbers are in the tens of thousands or more. Bayada has not disclosed the total.

49. Bayada also submitted a copy of its notice to the California Attorney General, which has posted it publicly. *See* California Attorney General, Bayada Sample Notice, https://oag.ca.gov/system/files/Bayada%20-%20Sample%20Notice.pdf.

50. On information and belief, the Private Information taken in the Data Breach has been or will be sold, traded, or published on criminal marketplaces, and

remains in the hands of people who have no right to it and no intention of protecting it.

D. Bayada Waited 137 Days to Tell Anyone

51. Bayada discovered the Data Breach on March 2, 2026.

52. Bayada did not complete its review of the affected data until July 1, 2026 — 121 days later.

53. Bayada did not mail notice letters until on or about July 17, 2026 — **137 days after discovery**.

54. HIPAA's Breach Notification Rule required Bayada to notify each affected individual "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." 45 C.F.R. § 164.404(b); *see also* 45 C.F.R. §§ 164.400–414. Sixty days from March 2, 2026 was May 1, 2026. Bayada blew that deadline by more than ten weeks.

55. Bayada's delay was not excused by the length of its investigation. HIPAA's 60-day clock runs from discovery of the breach, not from completion of a data review. And nothing prevented Bayada from telling patients promptly that their information had been taken while it worked out the details of exactly which fields were involved. Bayada chose to say nothing at all until it had finished.

56. The delay caused real, independent harm. Notice is the entire mechanism by which a breach victim can protect himself. During the 137 days of

Bayada's silence, Mr. Monaco and Class Members were not aware of the data breach, and therefore were not aware of the necessity to place fraud alerts or credit freezes, scrutinize their Explanation of Benefits statements for fraudulent claims, watch for accounts opened in their names, or enroll in monitoring. Meanwhile, the person who took their information had a free and unmonitored head start.

57. Bayada's notice letter also failed to give Plaintiff and Class Members the information they needed to assess their own risk. It did not say how the breach happened, how many people were affected, whether the data has appeared for sale, or what Bayada has done to secure its systems since. A notice that withholds the facts a victim needs is not meaningful notice.

E. What Bayada Offered Is Not Enough

58. Bayada offered affected individuals twelve months of credit monitoring, a credit report, and a credit score through Cyberscout, a TransUnion company, at https://bfs.cyberscout.com/activate, with a 90-day enrollment deadline.

59. That offer is inadequate in every dimension that matters.

60. **It is too short.** The information stolen in the Data Breach — dates of birth, diagnoses, Medicaid identification numbers, medical record numbers — does not become stale. It is valid for life. Criminals routinely hold stolen data for years before using it, precisely to outlast whatever monitoring the breached company paid

for. A twelve-month subscription against a lifetime risk is not a remedy; it is a gesture.

61. **It covers only one bureau.** Bayada's offer is limited to monitoring through a single credit reporting agency. Fraud reported to Experian or Equifax but not TransUnion would go undetected. A victim who relies on Bayada's offer is watching one of three doors.

62. **It monitors the wrong thing.** Credit monitoring is designed to catch new credit accounts. It is not designed to catch medical identity theft, fraudulent claims submitted to Medicaid under a stolen Medicaid identification number, prescriptions filled in a victim's name, or false entries inserted into a victim's medical file. Those are the most likely misuses of the specific data Bayada lost, and Bayada's offer does nothing about them. Medical identity theft is also uniquely dangerous, because corrupted medical records can lead to wrong treatment decisions later.

63. **It is out of reach for many of the people it was offered to.** Enrollment requires internet access and a working email address. Bayada's own notice states that the service "may not be available to minors under 18." Bayada provides pediatric home health care to children, and it provides care to adults who have been adjudicated incapacitated and cannot enroll themselves in anything. For Mr.

Monaco, enrollment is not something he can do; it is one more task that must be performed for him by a guardian.

64. **It shifts Bayada's burden onto its victims.** Bayada's notice instructs affected individuals to review their account statements and Explanation of Benefits forms, watch for signs of fraud, obtain credit reports, and consider fraud alerts and security freezes. Every one of those tasks costs time. Bayada created the need for that work by failing to secure the data and then failing to give timely notice. The cost of that work is a loss Bayada caused.

65. Retail identity and credit monitoring of the scope actually needed here costs hundreds of dollars per person per year, and would need to continue indefinitely.

F. Bayada Knew the Risk and Ignored It

66. The Data Breach was foreseeable. Health care providers have been among the most heavily targeted organizations in the country for years, and Bayada knew it.

67. The United States Department of Health and Human Services has repeatedly warned health care organizations about ransomware and data theft campaigns aimed at the sector, including published threat briefings describing the specific tactics used against health care providers. *See, e.g.*, U.S. Dep't of Health &

Human Servs., Royal & BlackCat Ransomware Threat Brief, https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf.

68. The Federal Bureau of Investigation and the United States Secret Service have publicly warned that hospitals and health care entities are attractive ransomware targets because they often have weaker IT defenses and a strong incentive to regain access to their data quickly.

69. The HHS Office for Civil Rights maintains a public portal cataloguing health care data breach affecting 500 or more individuals. *See* https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf. Hundreds of such breaches are reported every year. Bayada, a sophisticated national health care company with a compliance function and a designated Privacy Officer, was on notice of all of it.

70. Bayada was also on notice of the general explosion in data breaches. Independent reporting documented thousands of data breaches in recent years exposing over a billion sensitive records, with year-over-year increases in the hundreds of percent. *See* Identity Theft Resource Center, 2024 Data Breach Annual Report, https://www.idtheftcenter.org/publication/2024-data-breach-report/.

71. Given the sensitivity of what it held and the vulnerability of the people it served, Bayada's data security obligations were at the high end of the scale, not the low end. Bayada nonetheless failed to meet even a baseline standard.

G. Bayada Failed to Follow Well-Established Security Standards

72. Reasonable data security for an organization holding health information is not a mystery. It has been described in detail by federal regulators, federal agencies, and industry bodies for years.

73. HIPAA's Security Rule required Bayada, among other things, to: ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; protect against reasonably anticipated threats to the security of that information; protect against reasonably anticipated impermissible uses or disclosures; and ensure compliance by its workforce. 45 C.F.R. § 164.306(a)(1)–(4). It further required Bayada to implement a security management process to prevent, detect, contain, and correct security violations, 45 C.F.R. § 164.308(a)(1)(i); to regularly review records of information system activity, 45 C.F.R. § 164.308(a)(1)(ii)(D); and to implement technical access controls limiting electronic PHI to authorized persons, 45 C.F.R. § 164.312(a)(1). *See also* 45 C.F.R. §§ 164.302, 164.304, 164.306(e).

74. HIPAA's Privacy Rule required Bayada to have appropriate administrative, technical, and physical safeguards to protect the privacy of PHI, and to limit uses and disclosures to the minimum necessary. 45 C.F.R. § 164.530(b), (c)(1).

75. HIPAA's Breach Notification Rule required prompt notice, as described above. 45 C.F.R. §§ 164.400–414.

76. The Federal Trade Commission has long published guidance on reasonable data security, including *Protecting Personal Information: A Guide for Business*, which instructs companies to inventory the personal data they hold, keep only what they need, protect it with appropriate technical controls including encryption, restrict access, monitor for intrusions and unusual data flows, train employees, and dispose of data securely when it is no longer needed.

77. The FBI has published ransomware prevention guidance, and the Cybersecurity and Infrastructure Security Agency has published extensive guidance on network segmentation, patch management, multifactor authentication, and monitoring.

78. Widely accepted frameworks including the NIST Cybersecurity Framework, NIST Special Publication 800-53, NIST Special Publication 800-171, and the CIS Critical Security Controls set out the specific technical measures a reasonable organization holding sensitive data is expected to implement.

79. On information and belief, Bayada failed to comply with these standards. Among other failures, Bayada:

a. failed to implement adequate intrusion detection and monitoring, such that an unauthorized actor operated inside its network and copied data for approximately thirteen days without detection;

b. failed to implement adequate data loss prevention controls that would have flagged the mass exfiltration of patient files;

c. failed to encrypt or otherwise render unreadable the Private Information it stored, or failed to do so effectively;

d. failed to adequately segment its network so that a single point of compromise could not reach large volumes of patient data;

e. failed to implement adequate access controls limiting Private Information to those who needed it;

f. failed to adequately train its workforce, including its IT and security personnel, on reasonable cybersecurity practices;

g. failed to conduct adequate risk assessments, vulnerability scanning, and penetration testing;

h. failed to timely patch or remediate known vulnerabilities;

i. failed to adopt and follow a reasonable data retention and destruction policy, and instead retained the Private Information of former patients and former employees long past any legitimate need; and

j. failed to notify affected individuals promptly after discovering the Data Breach.

80. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits unfair practices in or affecting commerce. The FTC has brought enforcement actions establishing that a company's failure to employ reasonable measures to protect consumers' sensitive personal information is an unfair practice under Section 5, and the Third Circuit has confirmed the FTC's authority to police data security under that provision. *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

81. Bayada's failure to employ reasonable data security measures to protect the Private Information of its patients and employees constituted an unfair practice prohibited by Section 5 of the FTC Act.

82. Mr. Monaco and Class Members are within the class of persons that HIPAA, Section 5 of the FTC Act, and New Jersey's data security and notification statutes were enacted to protect, and the harm they suffered is the exact harm those laws were designed to prevent.

H. Stolen Health Information Is Valuable, Permanent, and Widely Misused

83. Private Information is a commodity. There is an established criminal market for it.

84. Health information commands a premium in that market. The Center for Internet Security has reported that the average cost per stolen record is roughly $158 across industries but approximately $355 in health care, and that protected health information can fetch up to approximately $363 per record.

85. A combination of a name, date of birth, and Social Security number has been reported to sell for approximately $60 to $80. Full identity profiles have been reported to sell for approximately $40 to $200, and stolen bank credentials for approximately $50 to $200. *See* Digital Trends, How Much Your Personal Data Costs on the Dark Web, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/. Entire breach datasets have been reported to sell for between roughly $999 and $4,995. *See* VPNOverview, In the Dark, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

86. HHS has warned that PHI "can be exceptionally valuable when stolen and sold" on criminal marketplaces, and has published analyses of the costs health care data breaches impose. *See* U.S. Dep't of Health & Human Servs., Cost Analysis of Healthcare Sector Data Breaches, https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf.

87. Medical identity theft is a substantial and growing share of all identity theft, and it is uniquely destructive. It can result in fraudulent charges, exhausted insurance benefits, denial of coverage, collection actions for care the victim never

received, and — most dangerously — false information entered into the victim's own medical record, which can lead to incorrect diagnoses and treatment.

88. A stolen Medicaid identification number is a direct tool for fraudulent billing. Combined with a diagnosis code, a procedure type, a payor authorization number, a treating physician's name, and a treatment location — all of which Bayada lost together for Mr. Monaco — it gives a criminal everything needed to submit claims that look legitimate.

89. Misuse is often delayed. The Government Accountability Office has reported that stolen data may not be used for months or years after a breach, and that the delay makes it difficult for victims to connect a later fraud to its source. *See* U.S. Gov't Accountability Office, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited, GAO-07-737, https://www.gao.gov/products/gao-07-737. The practical consequence is that the risk created by the Data Breach will persist long after Bayada's twelve months of monitoring expire.

90. Stolen data also compounds. Criminals combine data from multiple breaches to build fuller profiles, and use known details about a victim to make phishing and social engineering attempts far more convincing. A caller who already knows a patient's diagnosis, treating physician, and admission date is far more likely

to be believed. Elderly and incapacitated patients are especially vulnerable to exactly that kind of targeted approach.

91. Unlike a compromised payment card, none of this can be undone. Bayada cannot reissue Mr. Monaco's date of birth or his medical history.

I. Mr. Monaco's Injuries

92. As a direct and proximate result of the Data Breach, Mr. Monaco's Private Information — including his date of birth, diagnosis and diagnosis code, Medicaid identification, medical record number, payor authorization number, procedure type, subscriber member number, treating and referring physician, treatment cost information, treatment location, and admission date — was accessed and copied by an unauthorized person and is now outside of anyone's control.

93. Mr. Monaco suffered an invasion of his legally protected privacy interest in his own medical information. That invasion is complete; it happened the moment his files were copied.

94. Mr. Monaco has been placed at a present, substantial, and continuing risk of identity theft, medical identity theft, insurance and Medicaid fraud, and other misuse of his Private Information. That risk is not speculative: his information was deliberately targeted and taken by a criminal actor whose purpose in taking it was to exploit it.

95. Mr. Monaco's risk is worse than that of a typical breach victim in two respects. First, the data taken about him is medical and permanent, not financial and replaceable. Second, he is an adjudicated incapacitated person. He cannot monitor his own credit, cannot read his own Explanation of Benefits statements for fraudulent claims, cannot detect a prescription filled in his name, and cannot enroll himself in the monitoring Bayada offered. He is entirely dependent on others to protect him, which makes fraud against him both easier to commit and harder to catch.

96. Mr. Monaco suffered a loss in the value of his Private Information, which is a form of intangible property with recognized market value. Information that has been stolen and distributed to criminals is worth less to its owner than information that remains confidential.

97. Mr. Monaco did not receive the full benefit of the provider relationship. Bayada received Medicaid reimbursement through the Consolidated Waiver for services furnished to Mr. Monaco. Safe handling of the Private Information Bayada required and maintained was an integral incident of that provider relationship, including reasonable security and prompt notification. Bayada did not provide those protections.

98. Mr. Monaco will require credit monitoring, medical identity monitoring, and identity restoration services for the remainder of his life to address

the risk Bayada created. Bayada offered twelve months from one bureau. Because of the nature and permanence of the Private Information compromised in the Data Breach, Mr. Monaco will require reasonable protective measures beyond the limited monitoring offered by Bayada, including credit monitoring, medical identity monitoring, and identity restoration services.

99. Bayada's 137-day delay independently harmed Mr. Monaco by depriving him of the ability to take protective steps during the period when they would have mattered most.

100. Mr. Monaco retains a continuing interest in ensuring that the Private Information still in Bayada's possession is properly secured, and in having Bayada delete the information it no longer needs.

CLASS ACTION ALLEGATIONS

101. Plaintiff brings this action under Rules 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, as guardian of Angelo J. Monaco, and the following Class and Subclass:

- **Class:** All individuals residing in the United States whose Private Information was accessed, acquired, copied, or otherwise compromised in the data breach experienced by Bayada Home Health Care, Inc. between February 18, 2026 and March 2, 2026,

including all individuals to whom Bayada sent notice of that data breach.

- **Pennsylvania Subclass:** All members of the Class who are residents or citizens of the Commonwealth of Pennsylvania.

102. Excluded from the Class and Subclass are Bayada; its officers, directors, and legal representatives; the judge presiding over this action and the judge's immediate family and staff; and any person who timely and validly opts out.

103. Plaintiff reserves the right to modify or amend the Class and Subclass definitions, including to add subclasses, as this litigation proceeds and as discovery reveals additional facts.

104. **Numerosity — Rule 23(a)(1).** The Class is far too numerous for joinder to be practicable. Bayada reported more than 6,000 affected individuals in Vermont alone and more than 1,200 in Texas, and Bayada operates nationwide. The Class numbers in at least the thousands, and likely far more. The identity of Class Members is ascertainable from Bayada's own records, since Bayada mailed individualized notice letters to affected individuals.

105. **Commonality — Rule 23(a)(2).** There are numerous questions of law and fact common to the Class, including:

a. whether Bayada had a duty to protect the Private Information of Mr. Monaco and Class Members;

b. whether Bayada's data security measures were reasonable;

c. whether Bayada breached its duties;

d. how and when the unauthorized access occurred;

e. what categories of Private Information were compromised;

f. whether Bayada knew or should have known of the risk of a data breach;

g. whether Bayada failed to comply with HIPAA, Section 5 of the FTC Act, and applicable state data security and notification laws;

h. whether Bayada's notice was unreasonably delayed;

i. whether Bayada's notice was adequate in content;

j. whether Bayada retained Private Information longer than necessary;

k. whether Bayada entered into implied contracts with Plaintiff and Class Members and breached them;

l. whether Bayada owed and breached fiduciary duties;

m. whether Bayada invaded the privacy of Mr. Monaco and Class Members;

n. whether Bayada was unjustly enriched;

o. whether Bayada's conduct violated the Pennsylvania Unfair Trade Practices and Consumer Protection Law and the New Jersey Consumer Fraud Act;

p. whether Mr. Monaco and Class Members were injured and what the proper measure of damages is; and

q. whether Plaintiff and Class Members are entitled to injunctive and declaratory relief, and what that relief should require.

106. **Typicality — Rule 23(a)(3).** Plaintiff's claims are typical of the claims of the Class. Mr. Monaco's Private Information was compromised in the same Data Breach, taken from the same systems, by the same actor, during the same period, and he received the same form of delayed notice from Bayada. Plaintiff's claims arise from the same course of conduct and rest on the same legal theories as those of the Class.

107. **Adequacy — Rule 23(a)(4).** Plaintiff will fairly and adequately protect the interests of the Class. She has no interests antagonistic to or in conflict with the Class. She is a duly appointed guardian authorized to act on Mr. Monaco's behalf, and her co-guardian has consented to this action. She has retained counsel experienced in class action and data breach litigation who are competent to prosecute this action.

108. **Predominance and Superiority — Rule 23(b)(3).** Common questions predominate over any questions affecting only individual members. Bayada's conduct was uniform: a single intrusion into a single network, a single set of security failures, and a single delayed notification program. Whether that conduct was unlawful does not vary from Class Member to Class Member.

109. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The damages suffered by individual Class Members, while significant, are small relative to the expense and burden of individual litigation against a large corporate defendant. Most Class Members would have no practical ability to obtain redress on their own. Individual litigation would also risk inconsistent results and would waste judicial resources. Bayada's records make notice to the Class administratively straightforward.

110. **Injunctive Relief — Rule 23(b)(2).** Bayada has acted and refused to act on grounds generally applicable to the Class, making final injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole. Bayada continues to hold Class Members' Private Information under security practices that have already failed once.

111. **Issue Certification — Rule 23(c)(4).** In the alternative, Plaintiff seeks certification of particular issues, including whether Bayada owed a duty of care,

whether Bayada breached that duty, and whether Bayada's notice was unreasonably delayed.

112. Plaintiff is unaware of any difficulty in managing this action as a class action.

CLASS WIDE INJURY

113. Bayada's failure to implement and maintain reasonable data security, and its failure to give timely notice, injured Mr. Monaco and every Class Member in the same way and for the same reason: their Private Information was taken from Bayada, and they were not told in time to protect themselves.

114. As a result of Bayada's conduct, Mr. Monaco and Class Members have suffered and will continue to suffer damages, including:

a. invasion of privacy;

b. theft of their Private Information;

c. loss of the confidentiality of their protected health information;

d. present and continuing risk of identity theft, medical identity theft, and fraud;

e. lost time and lost opportunity costs spent detecting, preventing, contesting, and recovering from misuse of their Private Information;

f. out-of-pocket expenses incurred by Class Members for credit monitoring, medical identity monitoring, credit reports, credit freezes, identity restoration, and other reasonable mitigation measures;

g. diminution in the value of their Private Information;

h. loss of the benefit of the bargain with Bayada;

i. deprivation of the value of their Private Information, for which Bayada took no adequate steps to protect;

j. anxiety, emotional distress, and loss of peace of mind resulting from the exposure of their medical information;

k. continued risk to the Private Information that remains in Bayada's possession; and

l. future costs of remedying the harm caused by the Data Breach.

115. These injuries were reasonably foreseeable to Bayada. Bayada knew that a criminal who obtained patient files would attempt to exploit them, and that patients would bear the consequences.

116. The risk Bayada created is ongoing. On information and belief, Bayada continues to hold the Private Information of Mr. Monaco and Class Members, and has not demonstrated that it has corrected the failures that permitted the Data Breach.

Without injunctive relief, Mr. Monaco and Class Members face a real and immediate threat of repeated harm.

CAUSES OF ACTION

COUNT I — NEGLIGENCE
(On Behalf of Plaintiff and the Class)

117. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

118. Plaintiff brings this Count on behalf of herself, as guardian of Angelo J. Monaco, and the Class.

119. Bayada required Mr. Monaco, through Plaintiff, and Class Members to provide their Private Information as a condition of receiving care or employment, and it accepted, stored, and used that information.

120. By taking custody of that information, Bayada assumed a duty to exercise reasonable care to protect it. That duty arose from Bayada's special relationship with its patients, from Bayada's superior and exclusive knowledge of its own security practices, from the foreseeability of harm if the information were compromised, and from Bayada's own representations that it would protect the information.

121. Bayada's duty was informed and reinforced by HIPAA's Security, Privacy, and Breach Notification Rules; by Section 5 of the FTC Act; by New Jersey's data security and breach notification statutes; and by well-established

industry standards including the NIST Cybersecurity Framework and the CIS Critical Security Controls.

122. Bayada also had a duty to notify Plaintiff and Class Members promptly and fully upon discovering that their Private Information had been compromised, so that they could take steps to protect themselves.

123. Bayada also had a duty not to retain Private Information longer than reasonably necessary, and to securely destroy it thereafter.

124. Bayada breached each of these duties, as described above, including by failing to implement reasonable safeguards, failing to detect an intruder in its network for approximately thirteen days, failing to prevent the mass exfiltration of patient files, retaining data it no longer needed, and waiting 137 days after discovery to notify affected individuals.

125. Bayada's conduct also created an unreasonable risk of criminal misconduct by third parties. Where an actor's negligent conduct creates a foreseeable opportunity for a third party's criminal act, the actor is liable for the resulting harm. *See* Restatement (Second) of Torts § 302B.

126. Plaintiff and Class Members had no ability to protect themselves. They did not control Bayada's systems, could not evaluate Bayada's security, and were not told about the breach until months after it happened.

127. As a direct and proximate result of Bayada's breaches, Mr. Monaco and Class Members suffered the injuries and damages described above.

128. Bayada's conduct was, at a minimum, negligent, and its decision to delay notification for more than twice the period allowed by federal law, while its patients remained exposed, was reckless and in conscious disregard of the rights of Mr. Monaco and Class Members, warranting punitive damages.

129. Mr. Monaco and Class Members are entitled to compensatory damages, punitive damages, and injunctive relief.

COUNT II — NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

130. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

131. Plaintiff brings this Count on behalf of herself, as guardian of Angelo J. Monaco, and the Class.

132. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits unfair practices in or affecting commerce, including a company's failure to use reasonable measures to protect sensitive personal information. *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

133. HIPAA and its implementing regulations required Bayada to safeguard electronic protected health information and to provide breach notification without

unreasonable delay and no later than 60 days after discovery. 45 C.F.R. §§ 164.302, 164.304, 164.306, 164.308, 164.312, 164.400–414, 164.530.

134. New Jersey law required Bayada to disclose a breach of security to affected customers in the most expedient time possible and without unreasonable delay, N.J.S.A. § 56:8-163, and to destroy or render unreadable records containing personal information that are no longer to be retained, N.J.S.A. § 56:8-162.

135. Bayada violated each of these provisions.

136. These statutes and regulations were enacted to protect people like Mr. Monaco and Class Members — individuals whose sensitive personal and health information is held by others — from precisely the harm that occurred here: unauthorized disclosure of their information and the resulting risk of identity theft and fraud.

137. Bayada's violations constitue negligence per se.

138. As a direct and proximate result, Mr. Monaco and Class Members suffered the injuries and damages described above and are entitled to compensatory and punitive damages.

COUNT III — BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

139. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

140. Plaintiff brings this Count on behalf of herself, as guardian of Angelo J. Monaco, and the Class.

141. Plaintiff and Class Members entered into implied contracts with Bayada when they provided Mr. Monaco's and their Private Information in exchange for services or employment.

142. Bayada required the Private Information as a condition of the relationship, and it solicited and invited Plaintiff and Class Members to provide it.

143. In providing that information, Plaintiff and Class Members understood and intended that Bayada would use reasonable measures to protect it, would comply with its legal obligations regarding it, would notify them promptly if it were compromised, and would retain it only as long as necessary. Bayada's own privacy representations confirmed that understanding.

144. Bayada accepted the benefit of these implied contracts by receiving the Private Information, providing services, and collecting payment for those services from Plaintiff, Class Members, and their insurers and payors, including Medicaid. With respect to Mr. Monaco, Bayada received Medicaid reimbursement through the Consolidated Waiver for services furnished to him.

145. Plaintiff and Class Members would not have entrusted their Private Information to Bayada on the same terms had they known Bayada would fail to secure it and would delay notice for 137 days.

146. Plaintiff and Class Members fully performed their obligations.

147. Bayada breached the implied contracts by failing to implement reasonable data security, by failing to comply with its legal obligations, by retaining the information longer than necessary, and by failing to provide timely and adequate notice of the Data Breach.

148. As a direct and proximate result, Plaintiff and Class Members did not receive the benefit of their contractual or provider relationships with Bayada, and suffered the injuries and damages described above.

COUNT IV — BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

149. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

150. Plaintiff brings this Count on behalf of herself, as guardian of Angelo J. Monaco, and the Class.

151. Bayada stood in a relationship of trust and confidence with Plaintiff and Class Members. Bayada is a health care provider. It received its patients' most sensitive medical information for the specific and limited purpose of delivering care, and it did so with the understanding that the information would be kept confidential.

152. That relationship gave rise to a fiduciary duty to act in the best interests of Plaintiff, Mr. Monaco, and Class Members with respect to their Private Information, including a duty to keep it confidential, to protect it with reasonable

safeguards, to use it only for authorized purposes, to retain it only as long as necessary, and to disclose promptly any compromise of it.

153. Bayada's fiduciary duties were heightened here because a substantial portion of its patient population is elderly, seriously ill, disabled, minor, or legally incapacitated, and therefore especially dependent on Bayada and especially unable to protect itself.

154. Bayada breached its fiduciary duties by failing to safeguard the Private Information, by allowing it to be accessed and copied by an unauthorized actor, by retaining it beyond any legitimate need, and by concealing the Data Breach from Plaintiff and Class Members for 137 days.

155. As a direct and proximate result, Plaintiff and Class Members suffered the injuries and damages described above and are entitled to compensatory and punitive damages.

COUNT V — INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

156. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

157. Plaintiff brings this Count on behalf of herself, as guardian of Angelo J. Monaco, and the Class.

158. Mr. Monaco and Class Members had a legally protected privacy interest in their Private Information, including their diagnoses, medical records, treatment histories, insurance and Medicaid identifiers, and dates of birth.

159. Plaintiff and Class Members reasonably expected that this information would remain confidential and would be accessible only to Bayada and to those authorized to see it for purposes of care and payment. Bayada's own privacy notice reinforced that expectation.

160. Bayada's conduct resulted in the disclosure of that information to unauthorized third parties.

161. The disclosure of a person's medical diagnoses, treatment history, disability information, and Medicaid identifiers to criminals is highly offensive to a reasonable person.

162. Bayada acted with reckless disregard for the privacy of Mr. Monaco and Class Members by failing to implement basic safeguards for information it knew was highly sensitive and highly targeted, and by then concealing the compromise for 137 days.

163. As a direct and proximate result, Mr. Monaco and Class Members suffered an invasion of their privacy and the injuries and damages described above, and are entitled to compensatory and punitive damages.

COUNT VI — VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. §§ 56:8-1 et seq.
(On Behalf of Plaintiff and the Class)

164. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

165. Plaintiff brings this Count on behalf of herself, as guardian of Angelo J. Monaco, and the Class.

166. Bayada is headquartered in New Jersey, and the decisions and conduct at issue — how to secure patient data, how to respond to the Data Breach, and when and how to notify affected individuals — emanated from New Jersey. New Jersey law therefore applies to Bayada's conduct with respect to the Class.

167. The New Jersey Consumer Fraud Act ("NJCFA") declares unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate." N.J.S.A. § 56:8-2.

168. "Merchandise" under the NJCFA includes "any objects, wares, goods, commodities, services or anything offered, directly or indirectly to the public for sale." N.J.S.A. § 56:8-1(c). Bayada's home health care services are merchandise, and Plaintiff and Class Members are consumers.

169. Bayada violated N.J.S.A. § 56:8-2 by, among other things:

a. misrepresenting that it maintained policies and procedures that protect patients' personal health information;

b. omitting and concealing the material fact that its data security practices were inadequate and did not comply with HIPAA, Section 5 of the FTC Act, or industry standards;

c. concealing and failing to timely disclose the Data Breach for 137 days after discovering it;

d. issuing a notice letter that omitted material facts about the breach; and

e. engaging in unconscionable commercial practices by collecting and retaining highly sensitive medical information from a uniquely vulnerable population without securing it, and by offering an inadequate remedy after losing it.

170. Bayada also violated New Jersey's Identity Theft Prevention Act, N.J.S.A. §§ 56:8-161 to -166, which the Legislature enacted because identity theft victims "may lose job opportunities, may be refused loans, education, housing or cars, or even may get arrested for crimes they did not commit," and may "spend years repairing damage to credit histories."

171. The Data Breach was a "breach of security" within the meaning of N.J.S.A. § 56:8-161, because it involved unauthorized access to electronic files containing personal information that compromised the security, confidentiality, and integrity of that information.

172. N.J.S.A. § 56:8-163(a) required Bayada to disclose the breach to any affected customer who is a New Jersey resident "in the most expedient time possible and without unreasonable delay." N.J.S.A. § 56:8-163(c)(1) required Bayada to report the breach to the Division of State Police before disclosing it to customers. N.J.S.A. § 56:8-163(f) required Bayada, where more than 1,000 persons were affected, to notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

173. Bayada violated N.J.S.A. §§ 56:8-163(a), (c)(1), and (f) by failing to make the required disclosures in the most expedient time possible and without unreasonable delay, and on information and belief by failing to make the required reports to law enforcement and to all nationwide consumer reporting agencies.

174. N.J.S.A. § 56:8-162 required Bayada to "destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records

to make it unreadable, undecipherable or nonreconstructable through generally available means."

175. On information and belief, Bayada violated N.J.S.A. § 56:8-162 by retaining the Private Information of former patients and former employees indefinitely, long after any legitimate need for it had ended, and by failing to destroy or render unreadable records it no longer needed. Had Bayada complied, a substantial portion of the Private Information taken in the Data Breach would not have been in Bayada's systems to take.

176. A violation of N.J.S.A. §§ 56:8-162 and 56:8-163 constitutes an unlawful practice and a violation of the NJCFA. N.J.S.A. § 56:8-166.

177. Bayada's conduct was material and was intended to induce patients and their representatives to accept or continue Bayada's services, entrust Private Information to Bayada, and refrain from taking protective measures. With respect to Mr. Monaco, Plaintiff retained the right to reject Bayada and obtain authorized services from another qualified provider.

178. As a direct and proximate result of Bayada's unlawful practices, Plaintiff and Class Members suffered ascertainable losses, including the lost benefit of their bargain or provider relationship, diminution in the value of the services and protections received, economic losses associated with responding to the Data

Breach, and, as applicable to individual Class Members, reasonable mitigation and out-of-pocket expenses.

179. Plaintiff and Class Members are entitled to actual damages, treble damages, and reasonable attorneys' fees, filing fees, and costs under N.J.S.A. § 56:8-19, together with injunctive relief.

COUNT VII — UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class, Pleaded in the Alternative)

180. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

181. Plaintiff brings this Count on behalf of herself, as guardian of Angelo J. Monaco, and the Class.

182. This Count is pleaded in the alternative to Plaintiff's contract claims, in the event no contract is found to govern.

183. Plaintiff and Class Members conferred benefits on Bayada, including payments for services made directly or on their behalf, through insurers, and government payors including Medicaid, and including the Private Information itself, which has independent economic value.

184. Bayada knowingly accepted and retained those benefits.

185. Part of the consideration Bayada received was intended to be used to provide reasonable data security for the Private Information Bayada demanded and retained. Bayada did not provide it.

186. Instead, Bayada retained the money that should have been spent on adequate data security, and used it for its own benefit, thereby increasing its profits at the expense of Plaintiff and Class Members.

187. Bayada also obtained and retained the value of Mr. Monaco's and Class Members' Private Information without providing the security that was the condition of receiving it.

188. Under the circumstances, it would be inequitable and unjust for Bayada to retain these benefits without accounting for the value of the security obligations it allegedly failed to provide.. Plaintiff and Class Members received services and security materially inferior to what Bayada accepted compensation to furnish, and Bayada's failures caused them to suffer the injuries described above.

189. Plaintiff and Class Members are entitled to restitution and disgorgement of the amounts by which Bayada was unjustly enriched, and to the imposition of a constructive trust on those amounts.

COUNT VIII — DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

190. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

191. Plaintiff brings this Count on behalf of herself, as guardian of Angelo J. Monaco, and the Class.

192. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201–2202, this Court has authority to declare the rights and legal relations of the parties and to grant further necessary or proper relief.

193. An actual controversy exists between Plaintiff and Bayada concerning whether Bayada's data security practices comply with its legal duties, and whether Bayada's remedial measures are adequate.

194. Bayada continues to hold the Private Information of Mr. Monaco and Class Members. On information and belief, Bayada has not remediated the failures that permitted the Data Breach and has not adopted data security measures that satisfy its obligations. Plaintiff and Class Members therefore remain at risk of another breach of the same information.

195. Plaintiff seeks a declaration that:

a. Bayada's existing data security measures do not comply with its contractual, statutory, regulatory, and common law duties to protect the Private Information of Mr. Monaco and Class Members;

b. Bayada's failure to provide notice of the Data Breach within 60 days of discovery violated its obligations to Plaintiff and Class Members;

c. to comply with its duties going forward, Bayada must implement and maintain the reasonable data security measures described in the Prayer for Relief below; and

d. Bayada's offer of twelve months of single-bureau credit monitoring is inadequate to address the risk created by the Data Breach.

196. The requested declaratory relief will resolve the parties' dispute, will guide their future conduct, and will prevent further injury. Damages alone are an inadequate remedy, because the threat of another breach of the same permanent information is ongoing.

COUNT IX — VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 P.S. §§ 201-1 et seq.
(On Behalf of Plaintiff and the Pennsylvania Subclass)

197. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

198. Plaintiff brings this Count on behalf of herself, as guardian of Angelo J. Monaco, and the Pennsylvania Subclass.

199. The Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL") declares unlawful "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." 73 P.S. § 201-3.

200. Bayada's provision of home health care services to Pennsylvania residents, and its solicitation and handling of their Private Information in connection with those services, constitute "trade" and "commerce" within the meaning of 73 P.S. § 201-2(3).

201. Mr. Monaco obtained and received Bayada's home- and community-based services exclusively for personal, family, and household purposes through Pennsylvania's Consolidated Waiver. Bayada was identified through Mr. Monaco's supports-coordination and ISP process, but Plaintiff, acting as his guardian, retained the right to reject Bayada and obtain the authorized services from another qualified provider. Plaintiff accepted Bayada as the provider, Bayada furnished the authorized services specifically to Mr. Monaco, and Bayada received Medicaid reimbursement through the Consolidated Waiver for those services. Plaintiff alleges that this consumer-provider transaction, in which Medicaid functioned as the third-party payment mechanism, constitutes a purchase or lease of services within the meaning of 73 P.S. § 201-9.2.

202. Bayada engaged in unfair and deceptive acts and practices in violation of the UTPCPL, including 73 P.S. § 201-2(4)(v), (vii), and (xxi), by:

a. representing that it had policies and procedures in place that protect patients' personal health information, when its security practices were in fact unreasonable and inadequate;

b. representing, expressly and by implication, that its services had characteristics and benefits they did not have — namely, that patient information entrusted to Bayada would be securely maintained;

c. failing to disclose, and concealing, that its data security practices did not meet the requirements of HIPAA, Section 5 of the FTC Act, or industry standards, when it had a duty to disclose that material fact and when Plaintiff and the Pennsylvania Subclass could not have discovered it on their own;

d. failing to disclose the Data Breach in a timely manner, and instead concealing it for 137 days after discovery, in violation of the 60-day deadline imposed by 45 C.F.R. § 164.404(b);

e. providing a notice letter that omitted material facts necessary for recipients to evaluate their own risk, including how the breach occurred, how many people were affected, and what remedial measures Bayada had taken;

f. offering a remedy — twelve months of single-bureau credit monitoring — that Bayada knew or should have known was materially inadequate to address the lifetime risk arising from

stolen medical and Medicaid data, and that was structurally unavailable to portions of its own patient population; and

g. engaging in fraudulent and deceptive conduct that created a likelihood of confusion or misunderstanding about the security of patient information and the risks arising from the Data Breach.

203. Bayada's acts and practices were material. A reasonable consumer deciding whether and on what terms to entrust deeply personal medical information to a home health care provider would consider it important to know whether that provider actually secured the information and whether it would tell them promptly if something went wrong.

204. Plaintiff and the Pennsylvania Subclass justifiably relied on Bayada's representations and omissions concerning the security and confidentiality of their Private Information. Had Bayada disclosed the truth, they would not have provided their Private Information on the same terms, would have demanded additional protections, or would have taken steps to mitigate their exposure far earlier.

205. Bayada's conduct is ongoing and offends public policy, is immoral, unethical, oppressive, and unscrupulous, and caused substantial injury to consumers that they could not reasonably have avoided.

206. As a direct and proximate result of Bayada's unfair and deceptive acts and practices, Plaintiff and the Pennsylvania Subclass suffered ascertainable losses

of money and property, including the lost benefit of their provider relationships with Bayada, diminution in the value of the services and protections received, and, where incurred, reasonable costs associated with credit monitoring, medical identity monitoring, credit reports, freezes, identity restoration, and other mitigation measures.

207. Plaintiff and the Pennsylvania Subclass are entitled to actual damages, treble damages, statutory damages, injunctive relief, restitution, and reasonable attorneys' fees and costs under 73 P.S. § 201-9.2.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself as guardian of Angelo J. Monaco and on behalf of the Class and Pennsylvania Subclass, respectfully requests that the Court:

A. Certify the Class and the Pennsylvania Subclass under Rules 23(a), 23(b)(2), 23(b)(3), and, as appropriate, 23(c)(4) of the Federal Rules of Civil Procedure;

B. Appoint Plaintiff as Class Representative and appoint the undersigned as Class Counsel;

C. Enter judgment in favor of Plaintiff and the Class on all counts;

D. Award compensatory, consequential, statutory, treble, nominal, and punitive damages in amounts to be determined at trial;

E. Award restitution and disgorgement of Bayada's unjust enrichment, and impose a constructive trust as appropriate;

F. Award equitable, injunctive, and declaratory relief, including an order requiring Bayada to:

i. encrypt all Private Information it collects, stores, or transmits, both in transit and at rest, using industry-standard encryption;

ii. delete and purge all Private Information that Bayada no longer has a legitimate business or legal need to retain, and adopt and enforce a written data retention and destruction policy;

iii. design, implement, maintain, and monitor a comprehensive written information security program, subject to Court oversight, that complies with HIPAA and recognized industry frameworks including the NIST Cybersecurity Framework;

iv. engage qualified independent third-party security auditors and internal personnel to conduct testing, including simulated attacks, penetration tests, and audits, on

Bayada's systems on a periodic basis, and to promptly correct any problems or issues identified;

v. audit, test, and train its security personnel and its workforce regarding any new or modified procedures;

vi. segment its networks and databases so that Private Information is isolated from other data and from internet-facing systems, and so that a single compromise cannot reach the entire data store;

vii. implement and maintain continuous logging, intrusion detection, and data loss prevention monitoring sufficient to detect unauthorized access and mass exfiltration of data in real time;

viii. conduct regular database scanning and security checks, and promptly patch known vulnerabilities;

ix. cease storing Private Information in a cloud-based or other environment that has not been assessed and secured in accordance with recognized standards;

x. routinely and continually conduct internal training and education, at least annually, to inform internal security

personnel how to identify and contain a breach when one occurs, and what to do in response;

xi. implement a threat management program designed to appropriately monitor Bayada's information networks for threats, both internal and external;

xii. provide Plaintiff and Class Members with lifetime credit monitoring covering all three nationwide consumer reporting agencies, together with medical identity monitoring, insurance and Medicaid claims monitoring, and identity theft restoration services, at Bayada's expense, in a form that is accessible to minors and to persons under guardianship without requiring the affected individual to enroll personally;

xiii. disclose to Plaintiff and Class Members the full nature and scope of the Data Breach, including how it occurred, what categories of information were taken for each individual, how many individuals were affected, and what remedial measures Bayada has taken; and

xiv. educate Plaintiff and Class Members about the threats they face as a result of the Data Breach and the steps they must take to protect themselves;

G. Award Plaintiff and the Class pre-judgment and post-judgment interest as permitted by law;

H. Award reasonable attorneys' fees, costs, and expenses, including under 73 P.S. § 201-9.2 and N.J.S.A. § 56:8-19; and

I. Award such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all claims and issues so triable.

Dated: August 25, 2026

Respectfully submitted,

WOLF POPPER LLP

By: */s/* Adam T. Savett
Adam T. Savett
570 Lexington Avenue
New York, NY 10022
Tel: (212) 451-9655
Fax: (212) 486-2093
asavett@wolfpopper.com

KREHER & TRAPANI LLP

Francesco P. Trapani
100 East Penn Square, Suite 400
Philadelphia, PA 19107
Tel: (215) 907-7289
Fax: (215) 907-7287

frank@krehertrapani.com

Counsel for Plaintiff and the Proposed Class