UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION

PATRICIA CAVALLARO-KEARINS, on behalf of herself and all others similarly situated, Plaintiff, v. **MODERNIZING MEDICINE, INC.**, Defendant.	No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Patricia Cavallaro-Kearins ("Plaintiff"), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Modernizing Medicine, Inc. ("Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to her own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a medical software firm based in Boca Raton, Florida, that sells "AI solutions[.]"[1]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its current and former patients. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

[1] *Home Page*, MODMED, https://www.modmed.com (last visited Nov. 19, 2025).

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former patients' PII/PHI.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendant's failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, having received a breach notice from Defendant.[2] She brings this class action on behalf of herself, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former patients' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff is a natural person and a citizen of New York, where she intends to remain.

9. Defendant is a Delaware corporation with its principal place of business at 4850 T-Rex Avenue, Suite 200, Boca Raton, Florida 33431.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of

[2] *See* Plaintiff's Notice Letter, attached as **Exhibit A**.

interest and costs. Plaintiff and Defendant are citizens of different states, and there are over 100 putative Class Members.

11. This Court has personal jurisdiction over Defendant because it is headquartered in Florida, regularly conducts business in Florida, and has sufficient minimum contacts in Florida.

12. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiff and the Class

13. Defendant is a medical software firm based in Boca Raton, Florida, that sells "AI solutions[.]"[3]

14. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former patients.

15. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII/PHI.

16. Under state and federal law, businesses like Defendant have duties to protect its current and former patients' PII/PHI and to notify them about breaches.

17. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

a. "The security of Personal Information is important to us."[4]

[3] *Home Page*, MODMED, https://www.modmed.com (last visited Nov. 19, 2025).
[4] *Privacy Policy*, MODMED (Jan. 10, 2025) https://www.modmed.com/privacy-policy/.

b. "We use reasonable safeguards aimed to protect against unauthorized use, disclosure, alteration or destruction of the Personal Information we collect and maintain."[5]

Defendant's Data Breach

18. On October 17, 2025, Defendant sent Plaintiff and Class Members notice of data breach letters ("Notice Letter") providing them with notification of the Data breach.[6] Defendant revealed that on July 9, 2025, it was hacked in the Data Breach.[7] However, Defendant only "became aware" of its Data Breach on July 21, 2025.[8]

19. Worryingly, Defendant already admitted that the Data Breach impacted "data from some of our podiatry customers" and that "we learned on July 29, 2025, that an unauthorized third party was able to see and take copies of some information in the podiatry computer servers between July 9, 2025, and July 10, 2025."[9]

20. Because of Defendant's Data Breach, at least the following types of PII/PHI were compromised:

a. full names;

b. addresses;

c. dates of birth;

d. phone numbers;

e. email addresses;

---

[5] *Id*.
[6] *See* Ex. A. A sample copy of the Notice Letter can be viewed at https://ago.vermont.gov/sites/ago/files/documents/2025-10-17%20Modernizing%20Medicine%20Data%20Breach%20Notice%20to%20Consumers.pdf.
[7] Ex. A.
[8] *Id*.
[9] *Id*.

f. health insurance information;

g. medical information;

h. medical record numbers;

i. patient account numbers;

j. dates of service;

k. provider and practice names;

l. billing/diagnostic codes;

m. prescription/medication information; and

n. diagnosis and treatment information.[10]

21. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control.

22. However, the Data Breach impacted 737 individuals in Massachusetts alone.[11]

23. And yet, Defendant waited over until October 17, 2025. before it began notifying the class—a full 100 days after the Data Breach began.[12]

24. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

[10] *See Notice of Data Breach*, VERMONT ATTY GEN (Oct. 17, 2025) https://ago.vermont.gov/sites/ago/files/documents/2025-10-17%20Modernizing%20Medicine%20Data%20Breach%20Notice%20to%20Consumers.pdf.
[11] *Data Breach Notification Report*, MASS. OFF. CONSUM. AFFS. & BUS. REG. (Oct. 17, 2025) https://www.mass.gov/doc/data-breach-report-2025/download.
[12] *Notice of Data Breach*, VERMONT ATTY GEN (Oct. 17, 2025) https://ago.vermont.gov/sites/ago/files/documents/2025-10-17%20Modernizing%20Medicine%20Data%20Breach%20Notice%20to%20Consumers.pdf.

25. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

a. "Carefully review statements and explanations of benefits sent to you from your health care providers, insurance company, and financial institutions to ensure that all of your account activity is valid."[13]

b. "Report any questionable charges promptly to the provider or company with which you maintain the account."[14]

26. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

27. Since the breach, Defendant claims that "[w]e have further enhanced our security controls and practices as appropriate[.]"[15]

28. But such simple declarations are insufficient to ensure that Plaintiff's and Class Members' PII/PHI will be protected from additional exposure in a subsequent data breach.

29. Defendant has done little to remedy its Data Breach. And it appears that Defendant has not offered the Data Breach victims even rudimentary identity monitoring services.

30. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiff and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

---

[13] *Id.*
[14] *Id.*
[15] *Id.*

31. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully acquired data.

32. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[16]

33. Thus, on information and belief, Plaintiff's and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff's Experiences and Injuries

34. Plaintiff Patricia Cavallaro-Kearins received podiatric medical care from a healthcare provider that used Defendant's software.

35. Thus, Defendant obtained and maintained the PII/PHI of Plaintiff.

36. As a result, Plaintiff was injured by Defendant's Data Breach.

37. Plaintiff is very careful about the privacy and security of her PII/PHI. She does not knowingly transmit her PII/PHI over the internet in an unsafe manner. She is careful to store any documents containing her PII/PHI in a secure location.

38. Plaintiff provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

---

[16] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

39. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII/PHI.

40. Plaintiff received a Notice of Data Breach dated October 17, 2025.

41. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

42. Through its Data Breach, Defendant compromised Plaintiff's PII/PHI.

43. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

44. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

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

46. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

47. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

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

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

50. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Consumers Prioritize Data Security

51. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[17] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[18]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[19]

c. 89% of consumers stated that "I care about data privacy."[20]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[21]

---

[17] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited Nov. 19, 2025).
[18] *Id*. at 3.
[19] *Id*.
[20] *Id*. at 9.
[21] *Id*.

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[22]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[23]

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

52. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

[22] *Id*.
[23] *Id*. at 11.

h. continued risk to their PII/PHI—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

53. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

54. The value of Plaintiff and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

55. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

56. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

57. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

58. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this

Court or a jury, to find that Plaintiff and other Class Members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

59. Defendant disclosed the PII/PHI of Plaintiff and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiff and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

60. Defendant's failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

61. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

62. In 2024, a record 3,158 data breaches occurred—exposing approximately 1,350,835,988 sensitive records (i.e., 211% increase year over year).[24]

63. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have

[24] *2024 Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf.

lesser IT defenses and a high incentive to regain access to their data quickly."[25]

64. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations have experienced cyberattacks.[26]

65. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

66. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

67. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[27] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal 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.

---

[25] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[26] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Nov. 19, 2025).

[27] *Protecting Personal Information: A Guide for Business,* FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

68. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

69. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

70. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use 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.

71. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

72. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

73. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

74. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

75. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

76. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly

known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[28]

77. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[29]

78. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

[28] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[29] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

79. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

80. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3),

individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Modernizing Medicine, Inc. in July 2025, including all those individuals who received notice of the breach.

81. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

82. Plaintiff reserves the right to amend the class definition.

83. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

84. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

85. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 737 members.

86. Typicality. Plaintiff's claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

87. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. Her interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

88. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

89. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to

the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

90. Plaintiff incorporates by reference paragraphs 1–89 as if fully set forth herein.

91. Plaintiff and the Class (or their third-party agents) entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

92. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

93. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

94. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew

or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class Members' PII/PHI.

95. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII/PHI.

96. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

97. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

98. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

99. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship

arose because Plaintiff and the Class (or their third-party agents) entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

100. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII/PHI.

101. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class Members' sensitive PII/PHI.

102. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

103. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class Members' PHI.

104. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

105. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

106. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

107. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

108. Defendant breached these duties as evidenced by the Data Breach.

109. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

110. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

111. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

112. Defendant has admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

113. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

114. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

115. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

116. Plaintiff incorporates by reference paragraphs 1–89 as if fully set forth herein.

117. Plaintiff and Class Members either directly contracted with Defendant or Plaintiff and Class Members were the third-party beneficiaries of contracts with Defendant.

118. Plaintiff and Class Members (or their third-party agents) were required to provide their PII/PHI to Defendant as a condition of receiving services provided by Defendant. Plaintiff and Class Members (or their third-party agents) provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's services.

119. Plaintiff and Class Members (or their third-party agents) reasonably understood that a portion of the funds they paid would be used to pay for adequate cybersecurity measures.

120. Plaintiff and Class Members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

121. Plaintiff and the Class Members (or their third-party agents) accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for services.

122. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

123. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII/PHI.

124. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

125. After all, Plaintiff and Class Members (or their third-party agents) would not have entrusted their PII/PHI to Defendant (or their third-party agents) in the absence of such an agreement with Defendant.

126. Plaintiff and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

127. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

128. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

129. Defendant materially breached the contracts it entered with Plaintiff and Class Members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

130. In these and other ways, Defendant violated its duty of good faith and fair dealing.

131. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

132. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

133. Plaintiff and Class Members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

THIRD CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

134. Plaintiff incorporates by reference paragraphs 1–89 as if fully set forth herein.

135. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

136. Defendant owed a duty to its current and former patients, including Plaintiff and the Class, to keep this information confidential.

137. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class Members' PII/PHI is highly offensive to a reasonable person.

138. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

139. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

140. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

141. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

142. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

143. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

144. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

145. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

146. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for

monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiff and the Class.

147. In addition to injunctive relief, Plaintiff, on behalf of herself and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

148. Plaintiff incorporates by reference paragraphs 1–89 as if fully set forth herein.

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

150. Plaintiff and Class Members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their PII/PHI to provide services, and (2) accepting payment.

151. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members.

152. Plaintiff and Class Members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

153. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII/PHI.

154. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations

at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

155. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class Members' (1) PII/PHI and (2) payment because Defendant failed to adequately protect their PII/PHI.

156. Plaintiff and Class Members have no adequate remedy at law.

157. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

158. Plaintiff incorporates by reference paragraphs 1–89 as if fully set forth herein.

159. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII/PHI; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

160. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

161. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class Members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

162. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII/PHI.

163. Defendant also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

164. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

PRAYER FOR RELIEF

Plaintiff and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: November 19, 2025

Respectfully submitted,

/s/ Jeff Ostrow
Jeff Ostrow (FBN 121452)
Andrew Hausdorff (FBN 1068481)
KOPELOWITZ OSTROW P.A.
1 W. Las Olas Blvd., Ste. 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
ostrow@kolawyers.com
hausdorff@kolawyers.com

Mariya Weekes (FBN 56299)
MILBERG, PLLC
333 SE 2nd Avenue, Ste. 2000
Miami, FL, 33131
Telephone: (786) 206-9057
mweekes@milberg.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610

Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

**Pro hac vice forthcoming*
Attorneys for Plaintiff and Proposed Class

— EXHIBIT A —

ModMed

Return Mail Processing Center:
P.O. Box 1907
Suwanee, GA 30024

[redacted]

[redacted]
Patricia Cavallaro Kearins
[redacted]

October 17, 2025

Notice of Data Breach

Dear Patricia Cavallaro Kearins:

We are writing to inform you of an incident that may have involved your personal and/or health information. This letter is from Modernizing Medicine, Inc. ("ModMed"), which is a vendor that provides electronic health record and other services to podiatry providers, including New York Podiatric Medicine & Surgery P.C. from which you may have received care.

What happened?

On July 21, 2025, ModMed became aware of potential unauthorized activity in certain computer servers, which ModMed subsequently determined involved servers containing limited data from some of our podiatry customers. We immediately took steps to prevent any further unauthorized activity and began an investigation, including engaging a leading forensic firm. We also contacted law enforcement. Based on our review, we learned on July 29, 2025, that an unauthorized third party was able to see and take copies of some information in the podiatry computer servers between July 9, 2025, and July 10, 2025. We conducted a comprehensive data review of the impacted information to identify the affected practices and patients, and we notified affected health care providers beginning September 19, 2025.

What information may have been involved?

Based on the review, your personal information involved in this incident may have included one or more of the following: full name, address, date of birth, phone number, email address, health insurance information, and medical information (such as medical record number, patient account number, date(s) of service, provider and practice name, billing/diagnostic codes, prescription/medication information, and/or diagnosis and treatment information). **Your Social Security number, bank/financial account information, credit card information, driver's license number, government ID card, and full medical records were not involved in this incident.** Please note that not all data elements were involved for all individuals.

What we are doing

ModMed takes privacy and security very seriously. In response to this incident, we immediately took action to block and prevent further unauthorized activity. We have further enhanced our security controls and practices as appropriate to minimize the risk of a similar incident in the future.

[redacted]