Vicki J. Maniatis, Esq.
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Phone: (212) 594-5300
vmaniatis@milberg.com

[Additional Counsel on Signature Page]

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

RICHARD WEISS, individually and on behalf of all others similarly situated, Plaintiff, v. AFFILIATED DERMATOLOGISTS & DERMATOLOGIC SURGEONS, P.A., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY DEMAND**

Plaintiff Richard Weiss ("Plaintiff"), individually and on behalf of all others similarly situated, and on behalf of the general public, brings this Class Action Complaint, against defendant Affiliated Dermatologists & Dermatologic Surgeons, P.A. ("Affiliated Dermatologists" or "Defendant") based on personal knowledge and the investigation of counsel, and alleges as follows:

I. INTRODUCTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms they caused Plaintiff and similarly situated persons in the preventable data breach of Defendant's inadequately protected computer network.

2. On March 5, 2024, Affiliated Dermatologists identified unusual activity on certain systems within its computer network.[1] Following an investigation, Affiliated Dermatologists determined that cybercriminals infiltrated its insufficiently secured computer network and improperly accessed and acquired multiple sensitive files during the period March 2, 2024 through March 5, 2024 ("Data Breach" or "Breach").[2] The investigation further determined that the accessed and acquired files contained the unencrypted personal information of Plaintiff and Class members.[3]

3. According to Affiliated Dermatologists, the personal information accessed by cybercriminals involved a wide variety of personally identifiable information ("PII") and protected health information ("PHI"), including names, dates of birth, addresses, Social Security numbers, medical treatment information, health insurance information, driver's license numbers, and passport numbers (collectively, "Personal Information").[4] The data breach impacted 373,379 individuals.[5]

4. Affiliated Dermatologists provides dermatological services in various locations across New Jersey.[6]

5. As part of its business, Defendant obtained and stored the Personal Information of Plaintiff and Class members.

6. By taking possession and control of Plaintiff's and Class members' Personal Information, Defendant assumed a duty to securely store and protect the Personal Information of Plaintiff and the Class.

---

[1] *See* https://www.affiliateddermatologists.com/storage/app/media/24-05-20-updated-draft-substitute-notice-affiliated-dermatologist2971080371-1.pdf.

[2] *Id*.

[3] *Id.*

[4] *Id*.

[5] https://apps.web.maine.gov/online/aeviewer/ME/40/8a407012-92e1-4705-a2bd-2d388c523940.shtml.

[6] *See* https://www.affiliateddermatologists.com/medical/.

7. Defendant breached this duty and betrayed the trust of Plaintiff and Class members by failing to properly safeguard and protect their Personal Information, thus enabling cybercriminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

8. Defendant's misconduct – failing to implement adequate and reasonable measures to protect Plaintiff's and Class members' Personal Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that they did not have adequate security practices in place to safeguard the Personal Information, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiff and Class members across the United States.

9. Due to Defendant's failures, cybercriminals obtained and now possess everything they need to commit personal identity theft and wreak havoc on the financial and personal lives of thousands of individuals, for decades to come.

10. Plaintiff brings this class action lawsuit to hold Defendant responsible for its reckless failure to use statutorily required or reasonable industry cybersecurity measures to protect Class members' Personal Information.

11. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design or being negligent in the design, implementation, monitor, and maintaining reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9)

otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

12. As a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class members are now forced to deal with the danger of identity thieves possessing and using their Personal Information.

13. Additionally, Plaintiff and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

14. Plaintiff brings this action individually and on behalf of the Class and seeks actual damages and restitution. Plaintiff also seeks declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper.

II. THE PARTIES

15. Plaintiff Richard Weiss is a citizen and resident of Westchester County, New York.

16. Affiliated Dermatologists is a New Jersey Professional Association with its principal place of business in Morristown, New Jersey. Upon information and belief, the membership of Affiliated Dermatologists is comprised of members who are either New Jersey resident citizens or corporations.

III. JURISDICTION AND VENUE

17. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

18. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100

class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class are citizens of states that differ from Defendant.

19. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District, maintains its principal place of business in this District, and has sufficient minimum contacts this State.

20. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). Venue is further proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

IV. FACTUAL ALLEGATIONS

A. The Data Breach and Defendant's Belated Notice

21. Affiliated Dermatologists provides dermatological services in various locations across New Jersey.[7]

22. As part of its business, and to gain profits, Defendant obtained and stored the Personal Information of Plaintiff and Class members.

23. On March 5, 2024, Affiliated Dermatologists identified unusual activity on certain systems within its computer network.[8] Following an investigation, Affiliated Dermatologists determined that cybercriminals infiltrated its insufficiently secured computer network and improperly accessed and acquired multiple sensitive files during the period March 2, 2024 through March 5, 2024.[9] The investigation further determined that the accessed and acquired files contained the unencrypted personal information of Plaintiff and Class members.[10]

---

[7] *See* https://www.affiliateddermatologists.com/medical/.

[8] *See* https://www.affiliateddermatologists.com/storage/app/media/24-05-20-updated-draft-substitute-notice-affiliated-dermatologist2971080371-1.pdf.

[9] *Id.*

[10] *Id.*

24. According to Affiliated Dermatologists, the Personal Information accessed by cybercriminals involved a wide variety of PII and PHI, including names, dates of birth, addresses, Social Security numbers, medical treatment information, health insurance information, driver's license numbers, and passport numbers.[11] The Data Breach exposed the Personal Information of 373,379 individuals.[12]

25. Despite the breadth and sensitivity of the PII/PHI that was exposed, and the attendant consequences to patients as a result of the exposure, Affiliated Dermatologists failed to disclose the Data Breach or notified victims until months after the breach was identified. This delay further exacerbated the harms to Plaintiff and Class members.

26. Based on the notice letter received by Plaintiff, the type of cyberattack involved, and public news reports, it is plausible and likely that Plaintiff's Personal Information was stolen in the Data Breach.

27. Upon information and belief, the unauthorized third-party cybercriminal gained access to the Personal Information and has engaged in (and will continue to engage in) misuse of the Personal Information, including marketing and selling Plaintiff's and Class members' Personal Information on the dark web.

28. Accordingly, Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiff and Class members' Personal Information confidential and to protect such Personal Information from unauthorized access.

29. Indeed, Affiliated Dermatologist's Privacy Policy[13] assures:

> We are required by applicable federal and state laws ***to maintain the privacy of your protected health information***. We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning your protected health information. [Emphasis added.]

[11] *Id*.

[12] https://apps.web.maine.gov/online/aeviewer/ME/40/8a407012-92e1-4705-a2bd-2d388c523940.shtml.

[13] Available at: https://www.affiliateddermatologists.com/disclaimers/patientprivacy/.

30. Furthermore, upon information and belief, Affiliated Dermatologists provides every patient with a HIPAA compliant disclosure form in which it represents that it will protect patients' Personal Information.

31. Nevertheless, Defendant failed to spend sufficient resources on preventing external access, detecting outside infiltration, and training its employees to identify email-borne threats and defend against them.

32. For example, as evidenced by the Data Breach's occurrence, the infiltrated network was not protected by sufficient multi-layer data security technologies or effective firewalls.

33. Similarly, based on the delayed discovery of the Data Breach, it is evident that the infiltrated network, that Defendant allowed to store Plaintiff's Personal Information, did not have sufficiently effective endpoint detection.

34. Further, the fact that Personal Information was "accessed" in the Data Breach demonstrates that the Personal Information contained in the Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have accessed only unintelligible data.

35. Plaintiff and Class Members entrusted Defendant with sensitive and confidential information, including their Personal Information which includes information that is static, does not change, and can be used to commit a myriad of financial crimes.

36. The stolen Personal Information at issue has great value to the hackers, due to the large number of individuals affected and the fact the sensitive information that was part of the data that was compromised.

B. Plaintiff's Experience

37. In exchange for medical services, Plaintiff entrusted his Personal Information to Defendant. Pursuant to HIPAA, Affiliated Dermatologists was required to protect and maintain the confidentiality of Personal Information entrusted to it.

38. Plaintiff received a notice letter from Defendant dated May 23, 2024, informing him that his Personal Information—including his name, address, Social Security number, email, conditions, lab results, medications, treatment information, insurance information, claims information, and chart notes—was specifically identified as having been accessed and/or acquired by cybercriminals in the Data Breach.

39. Plaintiff is very careful with his personal information. To the best of his knowledge, he has never before had his Personal Information exposed in a data breach.

40. Plaintiff and Class members' Personal Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

41. Because of the Data Breach, Plaintiff's Personal Information is now in the hands of cyber criminals. Plaintiff and all Class members are now imminently at risk of crippling future identity theft and fraud.

42. As a result of the Data Breach, Plaintiff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, researching how best to ensure that he is protected from identity theft, reviewing account statements and other information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach. Defendant specifically advised Plaintiff to take these steps by providing a list of recommended "steps" for victims to take and further stating in the notice letter:

> We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity.[14]

43. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Personal Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's Personal Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Personal Information; and (e) continued risk to Plaintiff's Personal Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

C. Defendant had an Obligation to Protect Personal Information under the Law and the Applicable Standard of Care

44. Defendant also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[14] *See* Sample Breach Notice Letter, available at https://apps.web.maine.gov/online/aeviewer/ME/40/8a407012-92e1-4705-a2bd-2d388c523940.shtml.

45. Defendant is further required by various states' laws and regulations to protect Plaintiff's and Class members' Personal Information.

46. Defendant owed a duty to Plaintiff and the Class to design, maintain, and test its computer and application systems to ensure that the Personal Information in its possession was adequately secured and protected.

47. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees (and others who accessed Personal Information within its computer systems) on how to adequately protect Personal Information.

48. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a breach on its systems in a timely manner.

49. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

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

51. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

52. Defendant owed a duty of care to Plaintiff and the Class because Affiliated Dermatologists was a foreseeable victim of a data breach.

D. Defendant Fail to Comply with HIPAA Guidelines

53. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and

Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

54. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[15] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

55. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

56. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

57. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

58. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

59. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

[15] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

60. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

61. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

62. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[16]

[16] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

63. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

64. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

65. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[17] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[18]

E. Defendant was on Notice of Cyber Attack Threats and of the Inadequacy of their Data Security

66. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some

[17] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.

[18] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

of the biggest cybersecurity breaches: Target,[19] Yahoo,[20] Marriott International,[21] Chipotle, Chili's, Arby's,[22] and others.[23]

67. Defendant should certainly have been aware, and indeed was aware, that Affiliated Dermatologists was at risk for a data breach that could expose the Personal Information that it collected and maintained.

68. Defendant was also on notice of the importance of data encryption of Personal Information. Defendant knew it kept Personal Information in their systems and yet it appears Defendant did not encrypt these systems or the information contained within them.

F. Cyber Criminals Will Use Plaintiff's and Class Members' Personal Information to Defraud Them

69. Plaintiff and Class members' Personal Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune.

---

[19] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[20] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[21] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[22] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[23] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

70. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[24] For example, with the Personal Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[25] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

71. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[26]

72. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

73. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[27]

---

[24] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[25] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[26] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

[27] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*

74. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off the sale of Plaintiff's and the Class members' Personal Information on the dark web. The Personal Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

75. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[28]

76. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

77. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[30]

78. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

79. Victims of the Data Breach, like Plaintiff and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[31]

---

https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x- price-of-stolen-credit-card-numbers.html.

[28] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[29] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737.

[30] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[31] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

80. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

81. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal Information;

b. Improper disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

82. Moreover, Plaintiff and Class members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiff's and Class members' Personal Information.

83. Plaintiff and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the Personal Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Personal Information, Plaintiff and all Class members will need to have identity theft monitoring protection for the rest of their lives.

84. None of this should have happened. The Data Breach was preventable.

G. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' Personal Information

85. Data breaches are preventable.[32] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate

[32]Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

security solutions."[33] she added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[34]

86. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[35]

87. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

88. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.7 The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[36]

89. The FTC further recommends that companies not maintain Personal Information longer than is needed for authorization of a transaction; limit access to sensitive data; require

[33] *Id.* at 17.

[34] *Id.* at 28.

[35] *Id.*

[36] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2022).

complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

91. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

92. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

93. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

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

95. Defendant was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of Plaintiff's and Class Members' Personal Information.

96. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiff's and Class members' Personal Information.

97. Defendant was at all times fully aware of its obligation to protect the Personal Information of Plaintiff and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

98. Defendant maintained the Personal Information in a reckless manner. In particular, the Personal Information was maintained and/or exchanged, unencrypted, in Defendant's systems and were maintained in a condition vulnerable to cyberattacks.

99. Defendant knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would occur if Plaintiff's and Class members' Personal Information was stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of a breach.

100. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class members' Personal Information from those risks left that information in a dangerous condition.

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

V. CLASS ACTION ALLEGATIONS

102. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

103. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of the Nationwide Class, defined as follows:

> All persons residing in the United States whose Personal Information was compromised as a result of the Affiliated Dermatologists Data Breach.

104. Plaintiff also seeks to represent a New York Subclass defined as follows:

> All current and former patients of Affiliated Dermatologists residing in the New York whose Personal Information was compromised as a result of the Affiliated Dermatologists Data Breach.

105. The Nationwide Class and the New York Subclass are collectively referred to herein as the "Class."

106. Plaintiff reserves the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

107. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

108. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable.

109. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Personal Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiff's and Class members' Personal Information violated the FTC Act, and/or state laws and/or Defendant's other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Personal Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiff and the Class to use reasonable care in protecting their Personal Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Defendant continues to breach duties to Plaintiff and the Class;

j. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's actions or failures to act;

k. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class and the general public;

m. Whether Defendant's actions alleged herein constitute recklessness and a breach of Defendant's obligations; and

n. Whether Plaintiff and Class members are entitled to punitive damages.

110. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive Personal Information compromised in the same way by the same conduct of Defendant.

111. **Adequacy:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class that he seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

112. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

113. Class certification is proper under New Jersey Rule 4:32-1(b)(2), because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

114. Class certification is proper under New Jersey Rule 4:32-1(b)(3), because Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' Personal Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

115. A class action is superior to other available methods for the fair and efficient adjudication of the controversy.

116. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice letters by Defendant.

VI. CAUSES OF ACTION

COUNT ONE

NEGLIGENCE

117. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

118. Defendant gathered and stored the Personal Information of Plaintiff and Class Members as part of its business of soliciting its services to its patients and employees, which solicitations and services affect commerce.

119. Plaintiff and Class Members entrusted Defendant with their Personal Information with the understanding that Defendant would safeguard their information.

120. Defendant had full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiff and Class Members could and would suffer if the Personal Information were wrongfully disclosed.

121. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Personal Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

123. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

124. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiff or Class

Members of the Data Breach until months after learning that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiff and the Class.

125. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

126. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Personal Information, a necessary part of being patients at Defendant.

127. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Personal Information.

128. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

129. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Personal Information it was no longer required to retain pursuant to regulations.

130. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

131. Defendant had and continues to have a duty to adequately disclose that the Personal Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent,

mitigate, and repair any identity theft and the fraudulent use of their Personal Information by third parties.

132. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Personal Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

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

e. Failing to detect in a timely manner that Class Members' Personal Information had been compromised;

f. Failing to remove former patients' Personal Information it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

133. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Personal Information and not complying with applicable industry

standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

134. Plaintiff and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

135. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

136. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

137. The FTC has pursued enforcement actions against businesses, which, as a result of their failures to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

138. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

139. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Personal Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

140. Defendant has full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiff and the Class could and would suffer if the Personal Information were wrongfully disclosed.

141. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personal Information of Plaintiff and the Class, the critical importance of providing adequate security of that Personal Information, and the necessity for encrypting Personal Information stored on Defendant's systems.

142. It was therefore foreseeable that the failure to adequately safeguard Class Members' Personal Information would result in one or more types of injuries to Class Members.

143. Plaintiff and the Class had no ability to protect their Personal Information that was in, and possibly remains in, Defendant's possession.

144. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

145. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

146. Defendant has admitted that the Personal Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

147. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Personal Information of Plaintiff and the Class would not have been compromised.

148. There is a close causal connection between Defendant's failure to implement security measures to protect the Personal Information of Plaintiff and the Class and the harm, or

risk of imminent harm, suffered by Plaintiff and the Class. The Personal Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Personal Information by adopting, implementing, and maintaining appropriate security measures.

149. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Personal Information; (iii) lost or diminished value of Personal Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) Plaintiff's Personal Information being disseminated on the dark web; (x) nominal damages; and (xi) the continued and certainly increased risk to their Personal Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information.

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

151. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Personal Information, which remain in Defendant's possession and is subject to further unauthorized

disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Personal Information in its continued possession.

152. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

153. Defendant's negligent conduct is ongoing, in that it still holds the Personal Information of Plaintiff and Class Members in an unsafe and insecure manner.

154. Plaintiff and Class members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT TWO

BREACH OF IMPLIED CONTRACT

155. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

156. Plaintiff alleges this claim in the alternative to his breach of express contract claim.

157. Plaintiff and Class Members were required to provide Defendant with their Personal Information in order to receive medical care and treatment and/or to seek employment opportunities.

158. When Plaintiff and Class Members provided their Personal Information to Defendant when seeking medical services or employment, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their Personal Information and to timely notify them in the event of a Data Breach.

159. Based on Defendant's representations, legal obligations, and acceptance of Plaintiff's and the Class Members' Personal Information, Defendant had an implied duty to

safeguard their Personal Information through the use of reasonable industry standards. This implied duty was reinforced by Defendant's representations in its Privacy Policy.

160. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' Personal Information and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant months to warn Plaintiff and Class Member of their imminent risk of identity theft. Defendant also failed to notify Plaintiff and the Class Members whether or not their driver's license numbers were compromised, leaving Plaintiff and Class Members unsure as to the extent of the information that was compromised.

161. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiff's and the Class Members' Personal Information.

COUNT THREE

BREACH OF FIDUCIARY DUTY

162. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

163. At all relevant times hereto, Defendant owed, and owes, a fiduciary duty to Plaintiff and the Class, including its duty to keep Plaintiff and Class Members' Personal Information reasonably secure.

164. The fiduciary duty to patients is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530, which required Defendant to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient information and to secure the health care information it maintains and to keep it free from disclosure.

165. Defendant breached its fiduciary duty to Plaintiff by failing to implement sufficient safeguards and by disclosing Plaintiff's and other Class Members' Personal Information to unauthorized third parties.

166. As a direct result of Defendant's breach of its fiduciary duty of confidentiality and the disclosure of Plaintiff's confidential Personal Information, Plaintiff and the Class Members have suffered damages.

167. As a direct result of Defendant's breach of its fiduciary duty and the disclosure of Plaintiff's and Class Members' Personal Information, Plaintiff and the Class have suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, and humiliation.

168. Plaintiff and the other Class Members suffered and will continue to suffer damages including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii) improper disclosure of the Personal Information; (iii) loss of privacy; (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; (vii) loss of the benefit of the bargain; and (viii) emotional distress. At the very least, Plaintiff and the Class are entitled to nominal damages.

COUNT FOUR

UNJUST ENRICHMENT

169. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

170. Plaintiff and the Class bring this claim in the alternative to all other claims and remedies at law.

171. Through and as a result of Plaintiff and Class members' use of Defendant's services, Plaintiff and Class Members entrusted their Personal Information to Defendant. Thereby, Defendant received monetary benefits and the use of the valuable Personal Information for business purposes and financial gain.

172. Defendant collected, maintained, and stored the Personal Information of Plaintiff and Class members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it.

173. Defendant, by way of its affirmative actions and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on reasonable data privacy and security measures to secure Plaintiff's and Class members' Personal Information.

174. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Personal Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class members.

175. Defendant failed to implement—or adequately implement—data security practices, procedures, and programs to secure sensitive Personal Information, including without limitation those industry standard data security practices, procedures, and programs discussed herein.

176. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiff and Class members suffered and continue to suffer actual

damages, including (i) the amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's Personal Information, (ii) time and expenses mitigating harms, (iii) diminished value of Personal Information, (iv) loss of privacy, (v) harms as a result of identity theft; and (vi) an increased risk of future identity theft.

177. Defendant, upon information and belief, has therefore engaged in opportunistic and unethical conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class members' interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

178. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

COUNT FIVE

VIOLATIONS OF THE NEW YORK DECEPTIVE ACTS AND PRACTICES ACT N.Y. GEN. BUS. LAW § 349 ("GBL") (On Behalf of Plaintiff and the New York Subclass)

179. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

180. Plaintiff brings this claim on behalf of himself and the New York Subclass (referred to as the "Class" for this section).

181. Affiliated Dermatologists violated New York's General Business Law § 349(a) when it engaged in deceptive, unfair, and unlawful trade, acts, or practices in conducting trade or commerce and through furnishing of services, including but not limited to:

a. Misrepresenting material facts to Plaintiff and the Class by stating it would, *inter alia*, "maintain the privacy of your protected health information";[37]

b. Misrepresenting material facts, including by representing itself as a business that would comply with state and federal laws pertaining to the privacy and security of Personal Information belonging to Plaintiff and the Class;

c. Omitting and/or concealed material facts regarding its inadequate privacy and security protections for Personal Information belonging to Plaintiff and the Class;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain sufficient privacy and security related to Personal Information belonging to Plaintiff and the Class resulting in a data breach, which is in violation of duties imposed on Defendant by state and federal laws, including the Federal Trade Commission Act (15 U.S.C. § 45);

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiff and the Class in a timely and accurate manner, which violates duties imposed on Defendant by New York General Business Law § 899-aa(2).

182. Affiliated Dermatologists knew, or should have known, that its computer systems and security practices were inadequate to protect Personal Information entrusted to Affiliated Dermatologists by Plaintiff and the Class. Further, Affiliated Dermatologists knew, or should have known, that the risk of theft of Personal Information through a data breach was highly probable, particularly given that cybercriminals have increasingly targeted healthcare providers.

[37] https://www.affiliateddermatologists.com/disclaimers/patientprivacy/.

183. Affiliated Dermatologists was in a superior position to know the true facts regarding its deficient data security and should have disclosed this fact to the Plaintiff and the Class.

184. Affiliated Dermatologists mislead consumers regarding the security of its network and ability to secure Personal Information it collected by failing to disclose the true facts regarding its deficient data security. This constitutes false and misleading representation, which had the capability, tendency, and impact of deceiving or misleading consumers.

185. Affiliated Dermatologists' representations were material representations, which consumers such as Plaintiff and the Class relied upon to their detriment.

186. Affiliated Dermatologists' conduct is unconscionable, deceptive, and unfair, and is substantially likely to and did mislead consumers such as Plaintiff and the Class acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have been injured because they were not timely notified of the Data Breach causing their Personal Information to be compromised.

187. As a direct and proximate result of Affiliated Dermatologists' unconscionable, unfair, and deceptive acts and omissions, Plaintiff and the Class had their Personal Information disclosed to unauthorized third parties, which caused damage to Plaintiff and the Class.

188. Plaintiff and the Class seek relief under New York General Business Law § 349(h), including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and/or attorney's fees, expenses, and costs.

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seek the following relief:

a. An order certifying this action as a Class action;

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

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

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

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

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

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

COUNT SIX

DECLARATORY/INJUNCTIVE RELIEF

189. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

190. As previously alleged, Plaintiff and members of the Class entered into an implied contract that required Defendant to provide adequate security for the Personal Information it collected from Plaintiff and the Class.

191. Defendant owed a duty of care to Plaintiff and the members of the Class that requires it to adequately secure Personal Information.

192. Defendant still possesses Personal Information regarding Plaintiff and members of the Class.

193. Since the Data Breach, Defendant has announced few if any changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

194. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Personal Information in Defendant's possession is even more vulnerable to cyberattack.

195. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their Personal Information and Defendant's failure to address the security failings that lead to such exposure.

196. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

197. Plaintiff, therefore, seeks a declaration that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security and that to comply with its contractual obligations and duties of care, Defendant must implement and maintain additional security measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class

counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, restitution, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. Ordering that Defendant cease transmitting Personal Information via unencrypted email;

vi. Ordering that Defendant cease storing Personal Information in email accounts;

vii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

viii. Ordering that Defendant conduct regular database scanning and securing checks;

ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

x. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

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

DEMAND FOR JURY TRIAL

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

DATED: May 31, 2024

By: /s/ *Vicki J. Maniatis*
Vicki J. Maniatis, Esq.
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Phone: (212) 594-5300
vmaniatis@milberg.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Wills Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

**Pro Hac Vice application to be submitted*

Counsel for Plaintiff and the Proposed Class

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

RICHARD WEISS, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Westchester Cnty, NY
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Vicki J. Maniatis, Milberg Coleman Bryson Phillips Grossman, PLLC, 100 Garden City Plaza, Suite 500, Garden City, NY 11530; (212) 594-5300

DEFENDANTS

AFFILIATED DERMATOLOGISTS & DERMATOLOGIC SURGEONS, P.A.

County of Residence of First Listed Defendant Morris County, NJ
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

Not Known

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5000000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER 2:24-cv-06571

DATE
May 31, 2024

SIGNATURE OF ATTORNEY OF RECORD
/s/ Vicki J. Maniatis

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 12/09) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of New Jersey

RICHARD WEISS, individually and on behalf of all others similarly situated,

Plaintiff

v.

AFFILIATED DERMATOLOGISTS & DERMATOLOGIC SURGEONS, P.A.

Defendant

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* AFFILIATED DERMATOLOGISTS & DERMATOLOGIC SURGEONS, P.A.
Stephen W. Rosan, M.D., Registered Agent
182 South Street
Morristown, New Jersey 07960

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Vicki J. Maniatis
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

.

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: