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

**Counsel for Plaintiff and the Proposed Class*

[Additional Counsel Listed on Signature Page]

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

CHARLES ZISS, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	Case No. _____
v.	)	**JURY TRIAL DEMANDED**
AFFILIATED DERMATOLOGISTS & DERMATOLOGIC SURGEONS, P.A.	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Charles Ziss, ("Plaintiff"), through his undersigned counsel, brings this action against Defendant Affiliated Dermatologists & Dermatologic Surgeons P.A., ("Affiliated Dermatologists" or "Defendant") pursuant to the investigation of his counsel, personal knowledge as to himself and his own acts and otherwise upon information and belief, and alleges as follows:

INTRODUCTION

1. Defendant Affiliated Dermatologists & Dermatologic Surgeons P.A., is a healthcare provider with four office locations across Morris County and Somerset County, New Jersey.[1]

[1] *See* https://www.affiliateddermatologists.com/ (last accessed May 29, 2024)

2. On or about March 2, 2024, Affiliated Dermatologists experienced a hack and exfiltration of patient data, which it publicly reported on or about May 23, 2024 (the "Data Breach").

3. Affiliated Dermatologists reported that this Sensitive Personal Information ("SPI") included at least Name and Address, Date of Birth, Social Security Number, Email, Conditions, Lab Results, Medications, Treatment Information, Insurance Information, Claims Information and Chart Notes.

4. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

5. The information stole in cyber-attacks allows the modern thief to assume victims' identities when carrying out criminal acts such as the following:

- Filing fraudulent tax return
- Using the victim's credit history
- Making financial transactions on behalf of victims, including opening credit accounts in victims' names;
- Impersonating victims via mail and/or email
- Impersonating victims in cyber forums and social networks;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

6. Plaintiff and Class members' SPI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the SPI of Plaintiff and Class members.

7. As of this writing, there exist many class members who have no idea their SPI has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose SPI was compromised as a result of defendant's failure to: (i) adequately protect consumers' SPI, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates state statutes.

9. Plaintiff and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of SPI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under common law and state statutes; and (v) the continued and certainly an increased risk to their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is located within this District.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

13. Plaintiff Charles Ziss is a natural person residing in Somerset County, New Jersey. On or about May 23, 2024, Plaintiff Ziss was informed via a letter from Defendant that he had been a victim of the Data Breach.

14. Defendant, Affiliated Dermatologists & Dermatologic Surgeons, is a New Jersey Professional Corporation with its principal place of business in Morristown, New Jersey.

FACTUAL ALLEGATIONS

15. Defendant is a healthcare provider with associated facilities located in Morris County and Somerset County, New Jersey.

16. Defendant provides services to at least hundreds if not thousands of patients a year at its facilities.

17. In the ordinary course of doing business with Defendant, patients provide Defendant with SPI such as:

a. Contact and account information, such as name, usernames, passwords, addresses, telephone number, email address, and household members;

b. Authentication and security information such as government identification, Social Security number, security codes, and signature;

c. Demographic information such as age, gender, and date of birth;

d. Payment information, such as credit card, debit card, and/or bank account number; and

e. Medical history as self-reported by patients, or medical history as transmitted from other healthcare providers.

18. On or about May 23, 2024, Defendant issued letters to affected patients that it had detected that it was the target of a cybersecurity attack on its computer systems and that an unauthorized party gained access to the database that contained patient information.

19. While Defendant states that it became aware of the Data Breach on March 5, 2024, it took more than two months for Defendant to begin to notify victims of the breach.

20. As a result, Plaintiff and class members' SPI was in the hands of hackers for an as-yet unknown amount of time before Defendant began notifying them of the Data Breach.

21. Defendant maintains a HIPAA Policy on its web page noting various categories under which it may disclose treatment, payment, and healthcare information.[2] It lists several bases under which it may release protected health information without consent. However, releasing that information to hackers is not a disclosed category.

22. Defendant had obligations created by contract, industry standards, federal law, common law, state statute, and representations made to Plaintiff and Class members, to keep their SPI confidential and to protect it from unauthorized access and disclosure.

23. Plaintiff and Class members provided their SPI 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.

[2] *See* https://www.affiliateddermatologists.com/storage/app/media/notice20of20privacy20practices-1.pdf (last accessed May 29, 2024)

24. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the industry preceding the date of the breach.

25. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including the Defendant.

26. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[3] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[4]

27. The SPI of Plaintiff and members of the Class was taken by hackers to engage in identity theft and or to sell it to other criminals who will purchase the SPI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

28. Defendant knew, or reasonably should have known, of the importance of safeguarding the SPI of Plaintiff and members of the Class, including Social Security numbers, dates of birth, and other sensitive information, as well as of the foreseeable consequences that

[3] See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, (last accessed May 29, 2024)

[4] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Class as a result of a breach.

29. Plaintiff and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their SPI. The injuries to Plaintiff and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the SPI of Plaintiff and members of the class.

30. 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.

31. 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 networks' vulnerabilities; and implement policies to correct any security problems. 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.

32. The FTC further recommends that companies not maintain SPI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be

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

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

34. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer SPI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

35. Several industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

36. Best cybersecurity 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.

37. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity 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 established standards in reasonable cybersecurity readiness.

38. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

39. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

40. The SPI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[5]

41. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards

[5] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs, (last accessed May 29, 2024).

> and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[6]

42. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

43. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number. [7]

44. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[8]

---

[6] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf, (last accessed May 29, 2024).

[7] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft, (last accessed May 29, 2024).

[8] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf, (last accessed May 29, 2024).

45. If you receive a new Social Security number, you should not be able to use the old number anymore. For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[9]

46. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential SPI to mimic the identity of the user. The personal data of Plaintiff and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and members of the Class represents essentially one-stop shopping for identity thieves.

47. The FTC has released its updated publication on protecting SPI for businesses, which includes instructions on protecting SPI, properly disposing of SPI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

48. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in 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.[10]

[9] *Id*.
[10] See https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29, (last accessed May 29, 2024).

49. Companies recognize that SPI is a valuable asset. Indeed, SPI is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other SPI on a number of Internet websites. The stolen personal data of Plaintiff and members of the Class has a high value on both legitimate and black markets.

50. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

51. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent, and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

52. Based on the forgoing, 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, name, or date of birth.

53. 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.[11]

54. This is even more true for minors, whose Social Security Numbers are particularly valuable. As noted, there is extreme credit value in Social Security numbers that have never been used for financial purposes. It's relatively simple to add a false name, age or address to a Social Security number. After that happens, there is a window for thieves to open illicit credit cards or even sign up for government benefits.[12]

55. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

PLAINTIFF CHARLES ZISS'S EXPERIENCES

56. On or about May 23, 2024, Plaintiff Charles Ziss was informed, via the Notice Letter, that his private and personal information was leaked during the Data Breach. This information included Name and Address, Date of Birth, Social Security Number, Email, Medical Conditions, Lab Results, Medications, Treatment Information, Insurance Information, Claims Information and Chart Notes.

[11] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed May 29, 2024).

[12] https://cyberguy.com/security/identity-theft-scammers-target-innocent-children/ (last accessed May 29, 2024).

57. Plaintiff was a patient at Affiliated Dermatologist in 2018, at which time he provided his SPI to the Defendant.

58. Had Plaintiff Ziss known that his SPI would not have been adequately protected by Defendant, he would not have used Defendant's services, or he would have insisted that they not be stored in Defendant's system.

59. Since approximately April 1, 2024, Plaintiff Ziss has received numerous calls and text messages from various scammers purporting to offer various medical and medically related services. This activity indicates that his information has been placed into the hands of hackers and has already been sold throughout the dark web.

60. Additionally, Plaintiff is aware of no other source from which the theft of his SPI could have come. He regularly takes steps to safeguard his own SPI in his own control.

CLASS ACTION ALLEGATIONS

61. Plaintiff brings this nationwide class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

> All natural persons residing in the United States whose SPI was compromised in the Data Breach announced by Defendants on or about March 5, 2024 (the "Nationwide Class")
>
> All natural persons residing in New Jersey whose SPI was compromised in the Data Breach announced by Defendants on or about March 5, 2024 (the "New Jersey Subclass")

62. The New Jersey Subclass, together with the Nationwide Class, are collectively referred to herein as the "Classes" or the "Class".

63. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

64. Plaintiff reserves the right to modify or amend the definitions of the proposed Class and/or New Jersey Subclass before the Court determines whether certification is appropriate.

65. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has, as of this writing, indicated that the total number of Class Members is more than 370,000. The Classes are readily identifiable within Defendant's records.

66. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their SPI;

c. Whether Defendant Breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the SPI of Plaintiff and members of the

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of SPI belonging to Plaintiff and members of the Classes;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the SPI of Plaintiff and members of the Classes secure and to prevent loss or misuse of that SPI;

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

h. Whether Defendant Caused Plaintiff's and members of the Classes damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and members of the Classes that their SPI had been compromised;

j. Whether Plaintiff and the other members of the Classes are entitled to credit monitoring and other monetary relief;

k. Whether Defendant violated the New Jersey Consumer Fraud Act

67. **Typicality**: Plaintiff's claims are typical of those of the other members of the Classes because all had their SPI compromised as a result of the Data Breach due to Defendant's misfeasance.

68. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's counsel is competent and experienced in litigating privacy-related class actions.

69. **Superiority and Manageability:** Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

70. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as the New Jersey Subclass as a whole.

71. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their SPI;

b. Whether Defendant breached a legal duty to Plaintiff and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their SPI;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standard relating to data security;

d. Whether 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; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(By Plaintiff Individually and on Behalf of the Nationwide Class)

72. Plaintiff hereby re-alleges and incorporates by reference all of the allegations in paragraphs 1 to 71.

73. Defendant routinely handles SPI that is required of their patients, such as Plaintiff.

74. By collecting and storing the SPI of its patients, Defendant owed a duty of care to the individuals whose SPI it collected to use reasonable means to secure and safeguard that SPI.

75. As a medical provider, Defendant is aware of that duty of care to the SPI of its clients.

76. Additionally, as a covered entity, Defendant has a duty under HIPAA privacy laws to protect the confidentiality of patient healthcare information, including the kind stolen as part of the Data Breach.

77. Defendant has full knowledge of the sensitivity of the SPI and the types of harm that Plaintiff and Class Members could and would suffer if the SPI were wrongfully disclosed.

78. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their current and former patients' SPI, involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

79. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

80. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' SPI.

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

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

83. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' SPI, including basic encryption techniques freely available to Defendant.

84. Plaintiff and the Class Members had no ability to protect their SPI that was in, and possibly remains in, Defendant's possession.

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

86. Defendant had and continues to have a duty to adequately disclose that the SPI of Plaintiff and Class Members 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 Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their SPI by third parties.

87. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the SPI of Plaintiff and Class Members.

88. Defendant has admitted that the SPI of Plaintiff and Class Members was purposely exfiltrated and disclosed to unauthorized third persons as a result of the Data Breach.

89. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the SPI of Plaintiff and Class Members during the time the SPI was within Defendant's possession or control.

90. Defendant improperly and inadequately safeguarded the SPI of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

91. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former patients' SPI in the face of increased risk of theft.

92. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former patients' SPI.

93. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

94. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the SPI of Plaintiff and Class Members would not have been compromised.

95. There is a close causal connection between Defendant's failure to implement security measures to protect the SPI of Plaintiff and Class Members, and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class Members' SPI was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such SPI by adopting, implementing, and maintaining appropriate security measures.

96. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their SPI is used; (iii) the compromise, publication, and/or theft of their SPI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their SPI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI of its patients and former patients in its possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the SPI compromised as a result of the Data Breach for the remainder of Plaintiff's and Class Members' lives.

97. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their SPI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long

as Defendant fails to undertake appropriate and adequate measures to protect the SPI in its continued possession.

SECOND CLAIM FOR RELIEF
Invasion of Privacy
(By Plaintiff Individually and on Behalf of the Nationwide Class)

98. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 72.

99. Plaintiff and the Class had a legitimate expectation of privacy to their SPI and were entitled to the protection of this information against disclosure to unauthorized third parties.

100. Defendant owed a duty to Plaintiff and the Class to keep their SPI confidential.

101. Defendant failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted SPI of Plaintiff and the Class.

102. Defendant allowed unauthorized and unknown third parties access to and examination of the SPI of Plaintiff and the Class by way of Defendant's failure to protect the SPI.

103. The unauthorized release to, custody of, and examination by unauthorized third parties of the SPI of Plaintiff and the Class is highly offensive to a reasonable person.

104. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their SPI to Defendant as part of Plaintiff's and the Class's relationships with Defendant, but privately and with the intention that the SPI would be kept confidential and would be 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.

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

106. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

107. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

108. As a proximate result of the above acts and omissions of Defendant, the SPI of Plaintiff and the Class was disclosed to third parties without authorization, causing Plaintiff and the Class to suffer damages.

123. 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 in that the SPI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

THIRD CLAIM FOR RELIEF
Breach of Confidence
(By Plaintiffs Individually and On Behalf of the Nationwide Class)

124. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 72.

125. At all times during Plaintiff's and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class's SPI that Plaintiff and the Class provided to Defendant.

126. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class's SPI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

127. Plaintiff and the Class provided their SPI to Defendant with the explicit and implicit understanding that Defendant would protect and not permit the SPI to be disseminated to any unauthorized third parties.

128. Plaintiff and the Class also provided their SPI to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that SPI from unauthorized disclosure.

129. Defendant voluntarily received in confidence the SPI of Plaintiff and the Class with the understanding that their SPI would not be disclosed or disseminated to the public or any unauthorized third parties.

130. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the SPI of Plaintiff and the Class was disclosed and misappropriated to unauthorized third parties beyond Plaintiff and the Class's confidence, and without their express permission.

131. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

132. But for Defendant's disclosure of Plaintiff's and the Class's SPI in violation of the parties' understanding of confidence, their SPI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and the Class's SPI as well as the resulting damages.

133. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class's PII and

PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class's SPI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class's SPI.

134. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to decide how their SPI is used; (iii) the compromise and/or theft of their SPI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their SPI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their SPI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the SPI of Plaintiff and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of their SPI as a result of the Data Breach for the remainder of Plaintiff's and the Class Members' lives.

135. As a direct and proximate result of Defendant's breaches of confidence, 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.

FOURTH CLAIM FOR RELIEF
Violation of the New Jersey Consumer Fraud Act,
N.J.S.A. § 56:8-1, *et seq*.
(By Plaintiff Individually and on Behalf of the New Jersey Subclass)

136. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 72 and brings this claim on behalf of himself and the New Jersey Subclass (the "Class" for the purposes of this count).

137. Defendant has violated N.J.S.A. § 56:8-1*, et seq*., by engaging in unconscionable, deceptive, or fraudulent business acts and practices and omissions regarding the same as defined in N.J.S.A. § 56:8-2 with respect to the services provided to the Class.

138. Defendant engaged in unconscionable acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the SPI of Plaintiff and the Class with knowledge that the information would not be adequately protected; and by storing the SPI of Plaintiff and the Class in an unsecure environment in violation of HIPAA and the rules and regulations promulgated thereunder, including 42 U.S.C. § 1301, *et seq*., 45 C.F.R. §§ 164.400-414, and 45 C.F.R. § 164.306, *et seq*. (as alleged *supra*.); and in violation of the Federal Trade Commission Act, 15 U.S.C. § 45 and 17 C.F.R. § 248.201, which require Defendant to employ reasonable methods of safeguarding the PII and PHI of Plaintiff and the Class.

139. Further, Defendant failed to inform Plaintiff and the New Jersey Subclass that it had not undertaken sufficient measures to ensure the security of their SPI.

140. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiff's and the Class's legally protected

interest in the confidentiality and privacy of their SPI, nominal damages, and additional losses as described above.

141. Defendant knew or should have known that its data security practices were inadequate to safeguard the SPI of Plaintiff and the Class and that the risk of a data breach or theft was highly likely, especially given its inability to adhere to basic encryption standards and data disposal methodologies. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

142. Plaintiff and the Class seek relief under N.J.S.A. § 56:8-2.12 and §56-8.19 including, but not limited to, restitution to Plaintiff and the Class of money or property that Defendant may have acquired by means of Defendant's unconscionable business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unconscionable business practices, treble damages, declaratory relief, attorneys' fees and costs and injunctive or other equitable relief.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment, in the Alternative
(By Plaintiff Individually and on Behalf of the Nationwide Class)

143. Plaintiff and the Class hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 through 72.

144. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of storing their SPI with Defendant in such a way that saved expense and labor for Defendant.

145. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefited from the receipt of Plaintiff's and Class Members' SPI, as this was used by Defendant to facilitate its core functions.

146. The benefits given by Plaintiff and Class Members to Defendant were to be used by Defendant, in part, to pay for or recoup the administrative costs of reasonable data privacy and security practices and procedures.

147. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount to be determined at trial.

148. Under principles of equity and good conscience, Defendant should not be permitted to retain a benefit belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members granted to Defendant or were otherwise mandated by federal, state, and local laws and industry standards.

149. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds or benefits it received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the Defendant and the following:

A. For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and their counsel as Class Counsel;

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

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

E. Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and,

J. Such other and further relief as this court may deem just and proper.

K. Conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

M. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

N. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

O. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

P. For a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

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

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

S. For pre and post judgment interest on all amounts awarded; and

T. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

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

Dated: May 31, 2024

Respectfully Submitted,

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

John J. Nelson (*Pro Hac Vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Bryan L. Bleichner (*Pro Hac Vice* forthcoming)
Philip J. Krzeski (*Pro Hac Vice* forthcoming)
CHESTNUT CAMBRONNE, PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

**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

CHARLES ZISS, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff _____
(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

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

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

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

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

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 _____

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

CHARLES ZISS, 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: