UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

DAVID BERMAN, individually and on behalf of all others similarly situated, Plaintiff, v. AFFILIATED DERMATOLOGISTS AND DERMATOLOGIC SURGEONS, P.A., Defendant.	Case No. **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff David Berman ("Plaintiff") individually and on behalf of all others similarly situated, by and through their undersigned counsel, brings this Class Action Complaint against Affiliated Dermatologists and Dermatologic Surgeons, P.A ("Affiliated" or "Defendant"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Affiliated with sensitive personally identifiable information ("PII")[1] and protected health information ("PHI," and collectively with PII, "Private Information") that was impacted in a data breach (the "Data Breach" or the "Breach").

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it and its accompanying responsibility to store and transfer that information.

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

3. Affiliated is a dermatological healthcare practice with offices located in Morristown, New Jersey, Mt. Arlington, New Jersey, and Bridgewater, New Jersey.[2]

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on their affirmative representations to Plaintiff and the Class, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. Defendant failed to take precautions designed to keep its patients' and employees' Private Information secure. As a result, more than 380,000 of Defendant's patients' and employees Private Information was compromised in the Data Breach[3], including: (1) names, (2) dates of birth, (3) mailing addresses, (4) Social Security numbers, (5) driver's license numbers, (6) medical treatment information, and (7) health insurance information.[4]

6. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information it collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

7. Defendant admits that information in its system was accessed by unauthorized individuals, though it provided little information regarding how the Data Breach occurred.

8. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have

[2] *Home*, AFFILIATED DERMATOLOGISTS, https://www.affiliateddermatologists.com/ (last visited June 10, 2024).
[3] Breach Portal, U.S. Department of Health and Human Services, Office for Civil Rights (May 3, 2024) https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited June 10, 2024).
[4] Notice of Data Security Incident, Affiliated Dermatologists (Apr. 25, 2024), https://www.affiliateddermatologists.com/storage/app/media/pdf-file/24-05-01Updated-Draft-Substitute-Notice-Affiliated-Dermatologist.pdf (Last visited June 10, 2024).

lost the ability to control their private information and are subject to an increased risk of identity theft.

9. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Private Information for Plaintiff and Class Members.

10. As a result of the Defendant's inadequate digital security, Plaintiff and Class Members' Private Information was exposed to criminals. Plaintiff and the Class have suffered and will continue to suffer injuries including: financial losses caused by misuse of Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

11. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

12. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence; unjust enrichment, breach of implied contract, breach of implied covenant of good faith and fair dealing, and invasion of confidence.

13. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

Plaintiff

14. Plaintiff David Berman is a citizen of New Jersey and resides in Morristown, New Jersey. Plaintiff Berman is a patient of Affiliated. On May 23, 2024, Defendant sent Plaintiff Berman a notice of Data Breach indicating his Private Information was compromised. As a consequence of the Data Breach, Plaintiff Berman has been forced to, and will continue to, invest significant time monitoring his accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, Plaintiff Berman is now subject to substantial and imminent risk of future harm. Plaintiff Berman would not have used Defendant's services had he known that it would expose his sensitive Private Information.

Defendant

15. Defendant is a New Jersey Professional Association with its principal place of business in Morristown, New Jersey. Defendant provides a range of medical and cosmetic services to patients, including skin cancer screenings, Mohs microsurgery, acne treatment, eczema treatment, phototherapy, Botox, chemical peels, and micro-needling[5]

JURISDICTION AND VENUE

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

[5] *Home*, AFFILIATED DERMATOLOGISTS, https://www.affiliateddermatologists.com/ (last visited June 10, 2024).

costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class Members.

17. This Court has personal jurisdiction over Defendant because Defendant is registered to do business, and maintains its principal place of business, in Morristown, New Jersey.

18. Venue is proper in these District under 28 U.S.C. § 1391(b)(2) because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendant

19. Defendant is a dermatological healthcare practice that provides a range of medical and cosmetic services to patients.[6]

20. In the ordinary course of its business practices, Defendant stores, maintains, and uses an individuals' Private Information.

21. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the Private Information collected from them would be kept safe, confidential, and that the privacy of that information would be maintained.

22. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

23. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ

[6] *Id.*

reasonable measures to protect Plaintiff and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

24. On or around March 5, 2024, Defendant detected unusual activity on several of its IT systems[7], and found a ransom note on it network indicating that its network had been breached and data was stolen.[8]

25. On April 10, 2024, Defendant's internal investigation determined that between March 2, 2024 and March 5, 2024, the unauthorized actor obtained access to certain systems and copied data from its IT network, including the personal information of patients and employees.[9]

26. On May 3, 2024, Defendant filed a notice of Data Breach with the U.S. Department of Health and Human Services Office for Civil Rights ("U.S. HHS") whereby Defendant indicated 380,000 individuals were impacted by the Data Breach.[10] In a notice of the Data Breach, Defendant states that the following types of Private Information were compromised in the Data Breach: (1) names, (2) dates of birth, (3) mailing addresses, (4) Social Security numbers, (5) driver's license numbers, (6) medical treatment information, and (7) health insurance information.[11]

27. Plaintiff's claims arise from Defendant's failure to safeguard Private Information provided by and belonging to its patients and failure to provide timely notice of the Data Breach.

28. Defendant failed to take precautions designed to keep their patients' and employees' Private Information secure.

---

[7] Notice of Data Security Incident, AFFILIATED DERMATOLOGISTS (last updated May 23, 2024) https://www.affiliateddermatologists.com/storage/app/media/pdf-file/24-05-01Updated-Draft-Substitute-Notice-Affiliated-Dermatologist.pdf (last visited June 10, 2024).

[8] Steven Adler, *New Jersey Dermatology Practice Suffers 380,000-Record Data Breach,* (May 15, 2024), https://www.hipaajournal.com/new-jersey-affiliated-dermatologists-breach/ (last visited June 10 2024).

[9] *Id.*

[10] Breach Portal, U.S. Department of Health & Human Services, Office for Civil Rights, (May 3, 2024), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (Last visited June 10, 2024).

[11] *Id.*

29. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

30. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify and Timely Report the Data Breach

31. Defendant admits that unauthorized third persons accessed its network systems.

32. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

33. Defendant was not only aware of the importance of protecting the Private Information that it maintains, as alleged, it promoted its capability to do so, as evident from its Privacy Policy.[12]

34. Defendant provides on its website that:

> **Our Legal Duty**
> 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. We must follow the privacy practices that are described in this notice while it is in effect. This notice takes effect April 14, 2003, and will remain in effect until we replace it.[13]

35. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

[12] See *Patient Privacy,* AFFILIATED DERMATOLOGISTS, https://www.affiliateddermatologists.com/disclaimers/patientprivacy/ (Last visited June 10, 2024).
[13] *Id.*

36. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[14] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present patients' and employees sensitive Personal Information.

37. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[15] Immediate notification of a Data Breach is critical so that those impacted can take measures to protects themselves.

38. Despite being aware of the Data Breach in March 5, 2024, Defendant did not notify Plaintiff until May 24, 2024, more than two months later.

D. The Harm Caused by the Data Breach Now and Going Forward

39. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[16]

40. The type of data that may have been accessed and compromised here – such as, full names and Social Security numbers – can be used to perpetrate fraud and identity theft. Social

[14] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited June 10, 2024).
[15] *Id.*
[16] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited June 10, 2024).

Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

41. Plaintiff and Class members face a substantial risk of identity theft given that their Social Security numbers, addresses, dates of birth, and other important Private Information were compromised in the Data Breach. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

42. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

43. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[17]

44. For example, when the U.S. Department of Justice announced their seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is their pervasiveness. As data breaches in the news continue to reveal, PII about employees, customers and the public are housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[18]

---

[17] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited June 10, 2024).

[18] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018) https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited June 10, 2024).

45. PII 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.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[20]

46. A compromised or stolen Social Security number cannot be addressed as simply as a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he 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."[21]

47. The Private Information compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[22]

48. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in

---

[19] *Id.*

[20] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited June 10, 2024).

[21] *Id.*

[22] *Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited June 10, 2024).

2019, resulting in more than $3.5 billion in losses to individuals and business victims.[23]

49. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[24] Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen.

50. As a result of the Data Breach, the Private Information of Plaintiff and Class Members have been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' Private Information.

---

[23] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited June 10 2024).

[24] *Id.*

51. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

52. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

53. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

54. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the Data Breach publicly announced by Defendant in May of 2024 (the "Nationwide Class").

55. Plaintiff also seeks certification of a New Jersey Subclass, defined as follows:

> New Jersey residents whose personal information was compromised in the Data Breach publicly announced by Defendant in May of 2024 (the "New Jersey Subclass").

56. Specifically excluded from the Nationwide Class and New Jersey Subclass (collectively, the "Class") are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

57. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

58. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

59. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates that the Class is comprised of hundreds of thousands of Class Members. The Class is sufficiently numerous to warrant certification.

60. Typicality of Claims (Rule 23(a)(3)): Plaintiff's claims are typical of those of other Class Members because, Plaintiff, like the unnamed Class members, had his Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

61. Adequacy of Representation (Rule 23(a)(4)): Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer class action litigation and who will prosecute this action vigorously.

62. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

63. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. 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;

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

c. Whether Defendant's storage of Class Member's Private Information was done in a negligent manner;

d. Whether Defendant's conduct was negligent;

e. Whether Defendant had a duty to protect and safeguard Plaintiff and Class Members' Private Information;

f. Whether Defendant's conduct violated Plaintiff and Class Members' privacy;

g. Whether Defendant took sufficient steps to secure its customers' Private Information;

h. Whether Defendant was unjustly enriched;

i. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

64. Information concerning Defendant's policies is available from Defendant's records.

65. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

66. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

67. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

68. Given that Defendant had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

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

70. Plaintiff brings this claim individually and on behalf of the Class Members.

71. Defendant knowingly collected, came into possession of, and maintained Plaintiff and Class Members' Private Information, and 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.

72. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff and Class Members' Private Information.

73. Defendant had, and continues to have, a duty to timely disclose that Plaintiff and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

74. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its patients' Private Information.

75. 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. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

76. 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 Private Information.

77. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff and Class Members' Private Information.

78. 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 Plaintiff and Class Members' Private Information;

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

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

79. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff and Class Members' Private Information within Defendant's possession.

80. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff and Class Members' Private Information.

81. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

82. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff and Class Members' Private Information.

In violation of the FTC guidelines, *inter alia,* Defendant did not protect the personal patient information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

83. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

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

85. It was foreseeable that the failure to adequately safeguard Plaintiff and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

86. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff and Class Members' Private Information to be compromised.

87. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

88. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

89. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs

associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; and future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach.

COUNT II
UNJUST ENRICHMENT
(On behalf of Plaintiff and All Class Members)

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

91. Plaintiff and Class Members conferred a benefit upon Defendant by using Defendant's services.

92. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff and Class Members' Private Information, as this was used for Defendant to administer its services to Plaintiff and the Class.

93. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class Members' services and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant or utilized its services had they known Defendant would not adequately protect their Private Information.

94. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

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

96. Plaintiff and the Class provided and entrusted their Private Information to Defendant. Plaintiff and the Class provided their Private Information to Defendant as part of Defendant's regular business practices.

97. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, and to keep such information secure and confidential, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class Members in its possession was secure.

98. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant with their Private Information in order for Defendant to provide services, for which Defendant is compensated. In exchange, Defendant agreed to, among other things, and Plaintiff and the Class understood that Defendant would: (1) provide services to Plaintiff and Class Members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' Private Information; and (3) protect Plaintiff and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

99. Implied in these exchanges was a promise by Defendant to ensure the Private Information of Plaintiff and Class Members in its possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiff and Class Members' Private Information.

100. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff and Class Members' Private Information to be accessed in the Data Breach.

101. Indeed, implicit in the agreement between Defendant and its patients was the obligation that both parties would maintain information confidentially and securely.

102. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class Members would provide their Private Information in exchange for services by Defendant. These agreements were made by Plaintiff and Class Members as Defendant's patients.

103. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' Private Information if it did not intend to provide Plaintiff and Class Members with its services.

104. Defendant was therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and/or use.

105. Plaintiff and Class Members accepted Defendant's offer of services and fully performed their obligations under the implied contract with Defendant by providing their Private Information, directly or indirectly, to Defendant, among other obligations.

106. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information.

107. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Private Information.

108. Defendant's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

109. Instead of spending adequate financial resources to safeguard Plaintiff and Class Members' Private Information, which Plaintiff and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching their implied contracts it had with Plaintiff and Class Members.

110. As a proximate and direct result of Defendant's breaches of their implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT IV
BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiff and All Class Members)

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

112. Defendant has violated the covenant of good faith and fair dealing by its conduct alleged herein.

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

114. Plaintiff and Class Members have complied with and performed all, or substantially all, of the obligations imposed on their conditions of services with Defendant.

115. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard its patients Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class

Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

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

COUNT V
INVASION OF CONFIDENCE
(On Behalf of Plaintiff and All Class Members)

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

118. At all times during Plaintiff and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff and the Class's Private Information that Plaintiff and the Class entrusted to Defendant.

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

120. Plaintiff and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

121. Plaintiff and the Class also entrusted Defendant with their Private Information the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

122. Defendant voluntarily received in confidence Plaintiff and the Class's Private Information with the understanding that Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

123. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff and the Class's Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff and the Class's confidence, and without their express permission.

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

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

126. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff and the Class's Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiff and the Class's Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff and the Class's Private Information.

127. 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) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud,

and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present 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 Private Information, 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 Private Information of current and former patients; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representatives of the Class and their counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) For pre-judgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of monetary relief; and

(g) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: June 11, 2024

Respectfully submitted,

LEVI & KORSINSKY, LLP

By: */s/ Courtney E. Maccarone*
Courtney E. Maccarone
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: cmaccarone@zlk.com

Counsel for Plaintiff

JS 44 (Rev. 07/16)

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

David Berman, individually and on behalf of others similarly situated

(b) County of Residence of First Listed Plaintiff Morris Cty., NJ
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, Email and Telephone Number)*

Levi &Korsinsky, LLP; 33 Whitehall Street, 17th Floor, New York, NY 10004; Telephone: (212) 363-7500

DEFENDANTS

Affiliated Dermatologists and Dermatologic Surgeon, P.A.

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

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

Attorneys *(If 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)*

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

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 840 Trademark

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
- ❒ 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)***:
Class Action Fairness Act, 28 U.S.C 1332(d)(2)

Brief description of cause:
Failure to safeguard sensitive personally identifiable information (PII)

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE See attached Addendum DOCKET NUMBER

DATE 06/11/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Courtney E. Maccarone

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 the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

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. When the petition for removal is granted, check this box.
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 statue.

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.