**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF WISCONSIN**

| | |
|---|---|
| LYNN ANDERSON, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>FOREFRONT DERMATOLOGY, S.C. and FOREFRONT MANAGEMENT, LLC,<br><br>Defendants. | Case No. 21-cv-891<br><br>**CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

Plaintiff Lynn Anderson ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to herself, and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendants Forefront Dermatology, S.C. and Forefront Management, LLC (together "Forefront" or "Defendants") and in support thereof alleges the following:

## NATURE OF THE ACTION

1. Plaintiff brings this class action individually and on behalf of all other individuals who had their sensitive personally identifying information—including but not limited to names, addresses, dates of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, provider names, and/or medical and clinical treatment information (collectively, "PII")—disclosed to unauthorized third parties during a massive intrusion into Forefront's IT network by unauthorized parties (the "Data Breach").

2. According to the breach notification letters Forefront is sending to impacted breach victims, including Plaintiff, Forefront identified an intrusion into its IT systems on June 4, 2021, and launched an investigation into the breach during which time it took its network offline. It then conducted an investigation which lasted until June 24, 2021. Following its investigation, Forefront

determined that unauthorized persons gained access to Forefront's IT network between the dates of May 28, 2021 and June 4, 2021, during which time, Forefront confirms, those unauthorized persons "accessed certain files" that contain sensitive PII.

3. As a result of the Data Breach, PII of approximately 2.4 million individuals has been exposed to unauthorized persons. The sensitive data of these individuals is now in the hands of criminals. This data commands high prices on the illegal black market (including on the dark web) for such stolen data. Indeed, the only incentive for criminals to steal this information is to profit from it by selling it on the dark web, where other criminals can purchase the data to commit all types of fraud against individuals whose information has been stolen.

4. Forefront learned of the Data Breach on June 4, 2021, but based upon its breach notice letter to Plaintiff, it waited over a month, until July 8, 2021, to notify impacted individuals.

5. Forefront is a large dermatology services group that operates in 21 states and the District of Columbia. As a large medical services provider, Forefront was well aware of the risks of a data breach inherent to inadequate data security measures. It had the resources to protect class members' PII from a breach and to timely notify victims of the Data Breach, but failed to do, and to ensure that class members' PII did not fall into the hands of unauthorized persons.

6. Forefront's failures to ensure the adequacy of its IT networks and systems, and that class members' sensitive PII was secured and protected fell, far short of its obligations to Plaintiff and class members' and their reasonable expectations for data privacy, jeopardized the security of Plaintiff's and class members' PII, and put Plaintiff and class members at serious risk of fraud and identity theft.

7. As a result of Forefront's conduct and the resulting Data Breach, Plaintiff's and millions of class members' privacy has been invaded, their PII is now in the hands of criminals, and they face a substantially increased risk of identity theft and fraud. Victims of the Data Breach have already been harmed by Forefront's data privacy and data security failures, and Plaintiff and class members have been exposed to an imminent risk of harm, given the highly sensitive nature of the exposed data.

8. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

## PARTIES

9. Plaintiff Lynn Anderson is a citizen of the commonwealth of Pennsylvania, and resides in Pittsburgh, Pennsylvania. On or about July 8, 2021, Forefront sent Plaintiff Anderson, and Plaintiff Anderson subsequently received, a letter identifying that her PII may have been impacted by the Data Breach. After receiving the breach notification letter, Plaintiff estimates that she has spent in excess of 100 hours taking steps to determine if she has been subjected to fraud as a result of the Data Breach, and to prevent potential fraud or identity theft. She has taken (and continues to regularly take) steps to remove her personal information from and opt out of public websites so that her name does not turn up in internet search engine search results, out of concern for her publicly available information being used in connection with the stolen PII to commit fraud or identity theft against her. Plaintiff also has been monitoring bank statements and credit card statements, and has gone through these statements in detail to see if she had been subjected to any fraudulent charges. Plaintiff also has been vigilant in monitoring her credit since the Data Breach.

10. Defendant Forefront Dermatology, S.C. is a dermatology services provider and Wisconsin services corporation with a principal place of business located at 801 York Street, Manitowoc, Wisconsin 54220.

11. Defendant Forefront Management, LLC is a Delaware corporation registered to do business in Wisconsin.

12. Defendants' registered agent for service is CT Corporation System, located at 301 S. Bedford Street, Suite 1 in Madison, Wisconsin 53703.

## JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332 because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00) and is a class action in which one or more class members are citizens of states different from Forefront.

14. The Court has personal jurisdiction over Forefront because Forefront has principal offices in Wisconsin, conducts significant business in Wisconsin, and/or otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in Wisconsin.

15. Venue properly lies in this district because, *inter alia,* Wisconsin has a principal place of business in this district; transacts substantial business, has agents, and is otherwise located in this district; and/or a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district.

## FACTUAL ALLEGATIONS

### A. Overview of Forefront Dermatology

16. Forefront Dermatology is a Wisconsin-based dermatology group. Forefront provides a host of dermatological treatments, including medical and cosmetic treatments, at locations across the United States.[1]

17. Per its website, Forefront operates "175+" locations in 21 states (Alabama, Arizona, Colorado, Florida, Georgia, Illinois, Indiana, Iowa, Kentucky, Maryland, Michigan, Minnesota, Missouri, Montana, New Jersey, North Carolina, Ohio, Oklahoma, Pennsylvania, Virginia, and Wisconsin), and Washington, D.C., and claims to employ or otherwise be affiliated with "195+" board-certified dermatologists.[2]

18. In connection with providing dermatology services, Forefront collects and stores sensitive medical and health information and records of patients, including Plaintiff and class members.

19. On its website, Forefront touts its commitment to data privacy, claiming that "Forefront Dermatology and its affiliates . . . respect your privacy and are committed to protecting

[1] FOREFRONT DERMATOLOGY, *Conditions & Treatments*, https://forefrontdermatology.com/conditions-treatments/ (last visited July 27, 2021).

[2] FOREFRONT DERMATOLOGY, https://forefrontdermatology.com; https://forefrontdermatology.com/location/ (last visited July 27, 2021).

it through our compliance with this policy."[3] It also discloses the type of information it collects via its website, and presumably from patients seeking services from Forefront:

> **Information Collected**
> Forefront Dermatology collects several types of information via the Website:
>
> - **Personal Information**: Forefront Dermatology may collect personal information that identifies you as an individual ("Personal Information") such as name, e-mail address, mailing address, phone number, age and or date of birth, gender, insurance information, health and medical information or other protected health information, account numbers, financial and payment information such as credit card information, and any other information you choose to provide us.[4]

20. Despite Forefront's assurances and claimed commitment to privacy, and as evidenced by the Data Breach, Forefront failed to adequately protect Plaintiff's and class members' PII.

**B. <u>The Data Breach</u>**

21. In July 2021, Forefront confirmed that it suffered a massive intrusion into its IT systems. It first learned of the Data Breach on June 4, 2021, and investigated the breach until June 24, 2021. It concluded that the Data Breach period of vulnerability was May 28 to June 4, 2021.

22. On its website, Forefront has created a dedicated website for the Data Breach.[5] Forefront's dedicated website states the following, in pertinent part:

> On June 24, 2021, Forefront Dermatology, S.C. and its affiliated practices concluded its investigation of an intrusion into its IT network by unauthorized parties and determined that the incident resulted in unauthorized access to certain files on its IT systems that contain patient information. The company first identified the intrusion on June 4, 2021, and immediately took its network offline to protect the

[3] FOREFRONT DERMATOLOGY, *Privacy Policy*, https://forefrontdermatology.com/privacy-policy/ (last visited July 27, 2021).

[4] *Id.*

[5] FOREFRONT DERMATOLOGY, *Notice of Data Security Incident*, https://forefrontdermatology.com/incidentnotice/ (last visited July 27, 2021).

> information it maintains and secure its systems. In addition it promptly launched an investigation and notified law enforcement.
>
> The investigation determined that unauthorized parties gained access to Forefront Dermatology's IT network between the dates of May 28, 2021 and June 4, 2021 and accessed certain files that contain information pertaining to some patients. This information may have included patient names, addresses, dates of birth, patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, accession numbers, provider names, and/or medical and clinical treatment information.

23. Although Forefront claims "[t]here is no evidence that patient Social Security numbers, driver's license numbers, or financial account / payment card information were involved in this incident,"[6] reports indicate that approximately 2.4 million individuals have potentially been impacted by the Data Breach and have had their sensitive medical and health records exposed.

24. Specifically, and according to Forefront's report to the United States Department of Health and Human Services Office for Civil Rights ("OCR"), Forefront has disclosed that sensitive records for 2,413,553 individuals may have been exposed during the Data Breach.[7]

25. The nature of the information disclosed during the Data Breach is highly sensitive. Forefront's breach notification letter indicates that impacted victims of the breach may have had the following information disclosed: "name in combination with your address, date of birth, patient account number, health insurance plan member ID number, medical record number, dates of service, provider names, and/or medical and clinical treatment information."

26. Forefront's report to OCR that more than 2.4 million individuals were potentially impacted during the Data Breach is at odds with Forefront's statement on its website that its "investigation found evidence that only a small number of patients' information was specifically involved . . . ."[8]

---

[6] *Id*. (emphasis in original).

[7] U.S. DPT. OF HEALTH AND HUMAN SERVICES, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited July 27, 2021).

[8] FOREFRONT DERMATOLOGY, *Notice of Data Security Incident*, https://forefrontdermatology.com/incidentnotice/ (last visited July 27, 2021).

27. Forefront's dedicated breach page acknowledges that victims or potential victims of the Data Breach are being notified by Forefront, but Forefront appears to be providing no assistance to these individuals. Instead, it suggests that breach victims undertake the chore of protecting their identities and preventing fraud, advising victims "to review the statements they receive from their health care providers and health insurance plan" and stating that "[i]f individuals see services they did not receive, they should contact the provider or health plan immediately."[9] Forefront further states, without more, that it "is enhancing its security protocols," and provides a toll-free response phone line so that aggrieved breach victims can call Forefront.[10]

28. Notably, Forefront does not appear to have offered to provide victims of the Data Breach with any financial assistance in the event of fraud, such as credit monitoring and identity theft preventions services, which is routinely offered by companies that suffer massive data breaches exposing sensitive health and other information.

**C. Forefront Had an Obligation to Protect PII**

29. Forefront had obligations, e.g., under HIPAA (42 U.S.C. § 1302d *et. seq.*) and based on industry standards, to keep Plaintiff's and class members' PII confidential and to protect it from unauthorized disclosures. Plaintiff and class members provided their PII to Forefront with the common sense understanding that Forefront would comply with its obligations to keep such information confidential and secure from unauthorized disclosures.

30. Forefront's data security obligations and promises were particularly important given the substantial increase in data breaches—particularly those in the healthcare industry—which were widely known to the public and to anyone in Forefront's industries.

31. Forefront failed to spend sufficient resources on data privacy risk management.

32. Forefront is an entity covered by HIPAA (45 C.F.R. § 160.102). As such, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part

[9] *Id.*

[10] *Id.*

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

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

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

35. HIPAA requires Forefront to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

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

37. HIPAA's Security Rule requires Forefront to do the following:

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

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

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

d. Ensure compliance by its workforce.

38. HIPAA also required Forefront to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

39. HIPAA also required Forefront to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

40. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Forefront to provide notice of the breach to each affected individual "without unreasonable delay and *in no case later than 60 days following discovery of the breach*."[11]

41. Forefront's security failures demonstrate that it failed to honor its duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data leaks, data breaches, and cyber-attacks;

b. Adequately protecting Plaintiff's and class members' PII;

c. Ensuring the confidentiality and integrity of electronic protected health information it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

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

f. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

[11] U.S. DEP'T OF HEALTH & HUMAN SERVICES, *Breach Notification Rule*, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited June 2, 2021) (emphasis added).

g. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

h. Protecting against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

i. Ensuring compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Training all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

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

43. As described before, Forefront is also required (by HIPAA, industry standards and various other states' laws and regulations) to protect Plaintiff's and class members' PII, and further, to handle any breach of the same in accordance with applicable breach notification statutes.

44. In addition to its obligations under federal and state laws, Forefront owed a duty to Plaintiff and class members whose PII was entrusted to Forefront to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession or entrusted to it from being compromised, lost, stolen, accessed, and/or misused by unauthorized persons. Forefront owed a duty to Plaintiff and class members to provide reasonable security, consistent with industry standards and requirements, and to ensure that its computer systems and

networks, and the personnel responsible for them, adequately protected the PII of Plaintiffs and class members.

45. Forefront owed a duty to Plaintiff and class members whose PII was entrusted to Forefront to:

a. design, maintain, and test its computer systems to ensure that the PII in Forefront's possession was adequately secured and protected;

b. implement processes that would detect a breach on its data security systems in a timely manner;

c. act upon data security warnings and alerts in a timely fashion;

d. disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from exfiltration because such an inadequacy would be a material fact in the decision to entrust PII with Forefront; and

e. disclose in a timely and accurate manner when data breaches occurred.

46. Forefront owed duties of care Plaintiff and class members because they were foreseeable and probable victims of any inadequate data security practices.

47. Forefront failed to carry these duties, causing harm to Plaintiff and class members.

**D. Impact of the Data Breach**

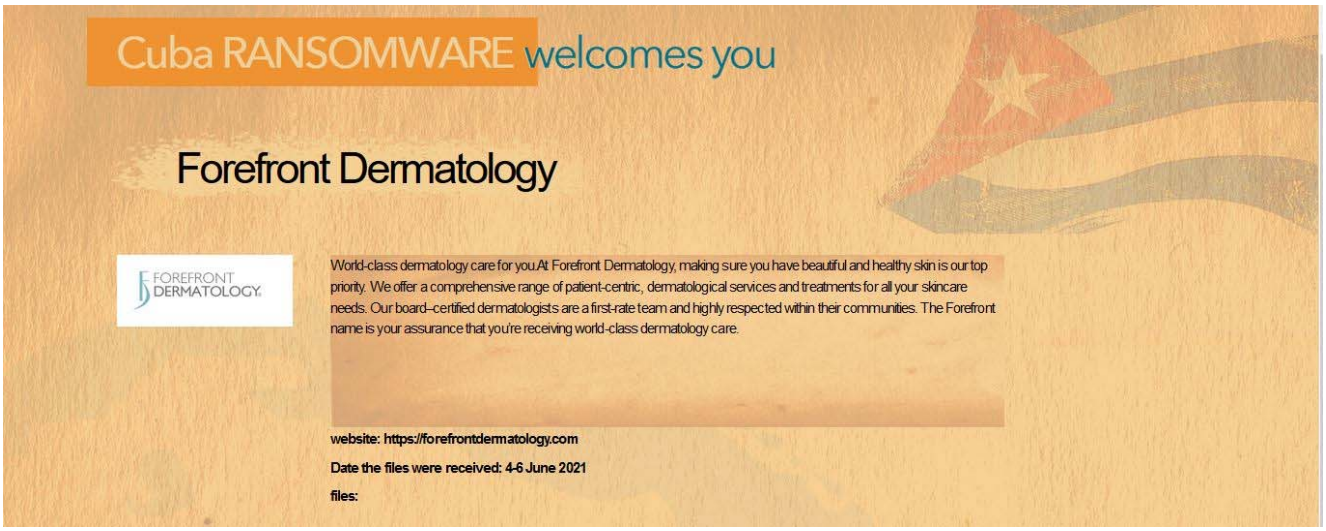
48. The actual extent and scope of the impact of the Data Breach remains uncertain. Unfortunately for Plaintiff and class members, the damage is already done. Their sensitive PII is now in the hands of unauthorized persons, and it is well known that a primary (if not the primary) purpose for criminals to steal sensitive information in a data breach is to monetize that data by selling it on the dark web or using it to commit fraud.

49. As a result of the Data Breach, in excess of 2.4 million people have reportedly had their sensitive PII exposed to criminals.

50. Although Forefront's public statements and dedicated breach webpage provide limited details about the nature or manner of the breach—i.e., whether it was a malware attack, a ransomware attack, if it was a ransomware attack, whether there was a ransom demand and whether

Forefront negotiated with the threat actors—information purporting to be from Forefront is apparently already available on the Cuba ransomware gang's leak site.

51. On information and belief, and based upon public reports, the Data Breach was the work of threat actors that call themselves the "Cuba Ransomware" gang. Reports indicate that "dumps" of Forefront data have surfaced on Cuba's website as of the end of June 2021. An image from that site is below[12]:




52. It is uncertain whether the Cuba site contains or relates to the same information stolen during the Data Breach, but it makes clear that Forefront's data privacy is inadequate, and that there is a large appetite for stolen sensitive information among cyber criminals.

53. The Data Breach creates a heightened security concern for Plaintiff and class members because sensitive health information was included. Forefront had a duty to keep Plaintiff's and other class members' PII confidential and to protect it from unauthorized disclosures. Plaintiff and class members provided their PII to Forefront, or entities affiliated with Forefront, with the

[12] DATABREACHES.NET, *Forefront Dermatology notifying patients and employees about ransomware incident* (July 12, 2021), https://www.databreaches.net/forefront-dermatology-notifying-patients-and-employees-about-ransomware-incident/.

understanding that the recipients of the sensitive PII would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

54. Forefront's data security obligations were particularly important given the substantial increase in data breaches—particularly those involving health information—in recent years, which are widely known to the public. Data breaches, especially ones involving sensitive health information, are by no means new and they should not be unexpected. These types of attacks should be anticipated by companies that collect and store sensitive PII, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks.

55. It is well known amongst companies that store sensitive PII that the information is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers …. Many of them were caused by flaws in . . . systems either online or in stores."[13]

56. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

57. There may be a time lag between when sensitive personal information is stolen and when it is used. According to the GAO Report:

> [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.[14]

[13] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[14] *Id*. at 29 (emphasis added).

58. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[15]

59. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen PII directly on various illegal websites making the information publicly available, often for a price.

60. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[16] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

61. Medical information and other PHI is especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[17] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

---

[15] *See* FEDERAL TRADE COMMISSION, WARNING SIGNS OF IDENTITY THEFT, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 3, 2021).

[16] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 A.M.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

[17] CLAIMS JOURNAL, *Study: Few Aware of Medical Identity Theft Risk*, (June 14, 2012), http://www.claimsjournal.com/news/national/2012/06/14/208510.htm.

62. A recent study also concluded the value of information available on the dark web sufficient to commit identity theft or fraud is about $1,010 per identity. The study identified that "[a] full range of documents and account details allowing identity theft can be obtained for $1,010."[18]

**E. Forefront Knew of the Risks of a Data Breach But Failed to Take Action**

63. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with data security standards.[19]

64. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Forefront failed to take reasonable steps to bolster its data security and adequately protect against the Data Breach and exposure of Plaintiff's and class members' PII, leaving patients and employees exposed to an imminent risk of fraud and identity theft.

65. The risk of harm is indeed imminent under the circumstances presented by the Data Breach. As the Seventh Circuit has noted, the Data Breach presents circumstances such that there is "no need to speculate as to whether [class members'] information has been stolen and what information was taken." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (citation omitted). In *Remijas,* 794 F.3d at 693, the Seventh Circuit explained how breach victims are harmed under the circumstances Forefront's patients and employees are facing:

> [T]he [impacted] customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an "objectively reasonable likelihood" that such an injury will occur. Requiring the plaintiffs "to wait for the threatened harm to materialize in order to sue" would create a different

[18] CISON, *You Are Worth $1,010 on the Dark Web, New Study by PrivacyAffairs Finds* (Mar. 8, 2021, 5:15 ET), https://www.prnewswire.com/news-releases/you-are-worth-1-010-on-the-dark-web-new-study-by-privacyaffairs-finds-301241816.html.

[19] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY.

> problem: "the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach." . . . At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the . . . data breach. *Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.*

(Emphasis added).

66. Forefront is, and at all relevant times has been, aware that the PII it collects in connection with providing dermatology services is highly sensitive, and it was aware of the importance of safeguarding that information and protecting its IT systems from security vulnerabilities.

67. Forefront was aware, or should have been aware, of regulatory and industry guidance regarding data security, and it was alerted to the risk associated with failing to ensure that PII was adequately secured.

68. Despite the well-known risks of hackers and cybersecurity intrusions, Forefront failed to employ adequate data security measures in a meaningful way, or make changes to its practices and protocols, in order to prevent breaches, including the Data Breach, impacting and exposing sensitive PII.

69. Had Forefront adequately protected and secured its IT systems and class members' PII, it could have prevented the Data Breach.

70. Forefront permitted Plaintiff's and class members' PII to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

71. As a result of the events detailed herein, Plaintiff and class members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; embarrassment and loss of privacy due to the exposure of sensitive PII, including sensitive health information; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of

value and loss of possession and privacy of PII; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of PII.

72. Plaintiff and class members now face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

## CLASS ALLEGATIONS

73. Plaintiff brings this action individually and on behalf of the following classes pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> **Nationwide Class**
> All residents of the United States whose PII was compromised in the Forefront Dermatology Data Breach that occurred between May 28, 2021 and June 4, 2021.
>
> **Pennsylvania Class**
> All residents of Pennsylvania whose PII was compromised in the Forefront Dermatology Data Breach that occurred between May 28, 2021 and June 4, 2021.

74. **Numerosity**: While the precise number of class members has not yet been determined, members of the classes are so numerous that their individual joinder is impracticable, as the proposed classes reportedly includes as many as 2.4 million geographically dispersed members.

75. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all class members were injured through Forefront's uniform misconduct, and Plaintiff's claims are identical to the claims of the class members they seek to represent. Accordingly, Plaintiff's claims are typical of class members' claims.

76. **Adequacy**: Plaintiff's interests are aligned with the classes Plaintiff seeks to represent and Plaintiff has retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and

Plaintiff's counsel intend to prosecute this action vigorously. Class members' interests are well-represented by Plaintiff and undersigned counsel.

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

78. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

- whether Forefront engaged in the wrongful conduct alleged herein;
- whether Forefront was negligent or negligent per se;
- whether Forefront breached implied contracts;
- whether Forefront's data security practices resulted in the disclosure of Plaintiff's and other class members' PII;
- whether Forefront violated privacy rights and invaded Plaintiff's and class members' privacy; and
- whether Plaintiffs and class members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

79. Given that Forefront engaged in a common course of conduct as to Plaintiff and the class members, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

## CAUSES OF ACTION

### COUNT I
### NEGLIGENCE

80. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

81. Forefront obtained sensitive PII from Plaintiff and class members, either directly or indirectly through third parties, in connection with providing dermatology and other health-related services.

82. Forefront was entrusted with, stored, and otherwise had access to the PII of Plaintiff and class members.

83. Forefront knew, or should have known, of the risks inherent to storing PII, and of the risks of not ensuring that the PII and its IT systems were secure. These risks were reasonably foreseeable to Forefront.

84. By collecting and maintaining PII, Forefront owed a duty of care to Plaintiff and class members who entrusted that information to Forefront to use reasonable means to secure and safeguard that information and to prevent disclosure to unauthorized individuals. That duty included a responsibility to implement processes by which Forefront could prevent IT intrusions, but also detect any data breach in a timely manner. As such, Forefront also had a duty to promptly notify Plaintiff and class members when the Data Breach occurred.

85. Forefront breached these duties by failing to provide fair, reasonable, or adequate data security, and by delaying providing notice of the Data Breach to impacted victims for many weeks.

86. Forefront's duty of care arises from its knowledge that class members entrust Forefront, directly or indirectly, with highly sensitive PII that Forefront is intended to, and represents that it will, handle securely. Forefront was in a position to ensure that its systems were sufficient to protect against a foreseeable risk that a data breach could occur, which would result in substantial harm to class members. Only Forefront was in a position to ensure that the data security measures

employed to protect its IT systems were sufficient to protect against breaches and the harms that Plaintiff's and class members have now suffered.

87. A "special relationship" also exists between Forefront, on the one hand, and Plaintiff and class members, on the other hand. Forefront entered into a "special relationship" with Plaintiff and class members by agreeing to accept, store, and have access to sensitive PII, including highly sensitive medical information, provided by them. Forefront was subject to an "independent duty" untethered to any contract between it and Plaintiff or any class members.

88. Forefront breached its duties through acts and omissions that include, but are not limited to:

a. failing to adopt, implement, and maintain adequate security measures to safeguard PII;

b. failing to adequately Forefront's IT systems for signs of intrusion;

c. allowing unauthorized access to Plaintiff's and class members' sensitive PII;

d. failing to detect in a timely manner that Plaintiff's and class members' sensitive PII had been compromised; and

e. failing to timely notify Plaintiff and class members about the Data Breach so that they could take appropriate steps to mitigate the risk of identity theft and other damages.

89. It was reasonably foreseeable to Forefront that its actions and omissions in failing to use reasonable measures to protect PII could result in injury to class members, creating a foreseeable zone of risk. The injury and harm suffered by Plaintiff and class members was the reasonably foreseeable result of Forefront's breaches of its duties.

90. Forefront acted with wanton disregard for the security of Plaintiff's and class members' PII. Plaintiff and class members have suffered, and continue to suffer, various types of harms as alleged above.

91. As a direct and proximate result of Forefront's negligent conduct, breach victims have suffered actual harm and face an increased and imminent risk of future harm.

92. As a direct and proximate result of Forefront's negligent conduct, Plaintiff and class members have suffered injury, or are reasonably certain to suffer injury, and are entitled to damages in an amount to be proven at trial.

93. Additionally, HIPAA and Section 5 of the FTC Act, 15 U.S.C. § 45, prohibit persons from engaging in unfair, abusive, or deceptive trade practices. The purpose of HIPAA and the FTC Act are, at least in part, to protect the interests of consumers who entrust their confidential data to companies like Forefront. Various FTC publications, regulations, and orders also form the basis of Forefront's duties.

94. Forefront had a duty to employ reasonable security measures under the HIPAA and Section 5 of the FTC Act, as interpreted and enforced by the FTC, including using reasonable measures to protect confidential PII, which it failed to do.

95. Forefront's duty to use reasonable care in protecting PII arose not only as a result of the statutes and regulations described above, but also because Forefront is bound by industry and regulatory standards to protect health information and other sensitive PII.

96. Forefront's actions and inactions in failing to use reasonable measures to protect PII and in failing to comply with applicable industry standards violated HIPAA and the FTC Act.

97. Forefront's acts and omissions caused the type of harm those laws were intended to prevent, namely, damages and injury due to unlawful consumer practices and divulging protected information.

98. Forefront's acts and omissions constituting violations of these laws are further evidence of Forefront's negligence, and actually and proximately caused the damages suffered by Plaintiff and the class members, as described herein.

99. Plaintiff and class members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

100. Plaintiff and Class members are also entitled to injunctive relief requiring Forefront to, *inter alia*: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all class members.

101. The overall public interest of ensuring the security of sensitive PII, including health and medical information, is furthered by the remedies sought herein. These remedies will compensate class members injured by Forefront's breach of its duties to them and will ensure that class members and future patients or employees of Forefront are protected from further breaches.

## COUNT II
## NEGLIGENCE PER SE

102. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

103. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Forefront had a duty to provide adequate data security practices in connection with safeguarding Plaintiff's and class members' PII.

104. Pursuant to HIPAA (42 U.S.C. § 1302d *et seq.*), Forefront had a duty to implement reasonable safeguards to protect Plaintiff's and class members' PII.

105. Forefront breached its duties to Plaintiff and class members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et. seq.*), and other statutes, by failing to provide fair, reasonable, or adequate data security in order to safeguard Plaintiff's and class members' PII.

106. Forefront's failure to comply with applicable laws and regulations constitutes negligence per se.

107. But for Forefront's wrongful and negligent breach of duties owed to Plaintiff and class members, Plaintiff and class members would not have been injured.

108. The injury and harms suffered by Plaintiff and class members were the reasonably foreseeable result of Forefront's breach of its duties. Forefront knew or should have known that it was failing to meet its duties, and that the Data Breach would cause Plaintiff and class members to experience the foreseeable harms associated with the exposure of their PII.

109. As a direct and proximate result of Forefront's negligent per se conduct, Plaintiff and class members now face an increased risk of future harm. As a direct and proximate result of Forefront's negligent per se conduct, Plaintiff and class members have suffered injury and are entitled to damages in an amount to be proven at trial.

## COUNT III
## BREACH OF IMPLIED CONTRACT

110. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

111. Forefront provided, directly or indirectly, dermatology and other related health, medical, and cosmetic services to Plaintiff and class members in exchange for payment.

112. In connection with receiving these health-related services, Plaintiff and class members entered into implied contracts with Forefront.

113. Pursuant to these implied contracts, Plaintiff and class members paid money to Forefront, whether directly or indirectly, and provided Forefront with, and Forefront received, their PII. In exchange, Forefront agreed, among other things: (1) to provide health-related services to Plaintiff and class members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and class members' PII; and (3) to protect Plaintiff's and class members' PII in compliance with federal and state laws and regulations and industry standards.

114. The protection of PII was a material term of the implied contracts between Plaintiff and class members, on the one hand, and Forefront, on the other hand. Indeed, Forefront recognized the importance of data privacy, and touted that it "respects" privacy in its website privacy policy

115. Had Plaintiff and class members known that Forefront would not adequately protect PII and that Forefront does not respect privacy, they would not have done business with Forefront.

116. Plaintiff and class members performed their obligations under the implied contracts when they provided Forefront with their PII and paid—directly or indirectly—for dermatological or other health-related services from Forefront.

117. Necessarily implicit in the agreements between Plaintiff/class members and Forefront was Forefront's obligation to take reasonable steps to secure and safeguard PII.

118. Forefront breached its obligations under the implied contracts with Plaintiff and class members by failing to implement and maintain reasonable security measures to protect their PII.

119. Forefront's breaches of its obligations under implied contracts with Plaintiff and class members directly resulted in the Data Breach and/or the exposure of Plaintiff and class members' PII to unauthorized persons.

120. The damages sustained by Plaintiff and class members were the direct and proximate result of Forefront's material breaches of these agreements.

121. Plaintiff and other class members were damaged by these breaches of implied contracts because: (i) they paid—directly or indirectly through insurance—for data security

protection they did not receive; (ii) they face a substantially increased and risk of fraud and identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established and burgeoning national and international market; and/or (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of fraud and identity theft they face and will continue to face.

## COUNT IV
## INVASION OF PRIVACY

122. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

123. Plaintiff and class members had a reasonable expectation of privacy in the PII that Forefront disclosed without authorization.

124. By failing to keep Plaintiff's and class members' PII safe, and disclosing PII to unauthorized parties for unauthorized use, Forefront unlawfully invaded Plaintiff's and class members' privacy right to seclusion by, *inter alia*:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

125. Forefront knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and class members' position would consider its actions highly offensive.

126. Forefront invaded Plaintiff's and class members' right to privacy and intruded into

their private affairs by disclosing their PII to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

127. By failing to keep Plaintiff's and class members' PII safe, and disclosing PII to unauthorized parties for unauthorized use, Forefront also unlawfully publicized private information of Plaintiff and class members.

128. Forefront publicized private PII to unauthorized persons during the Data Breach.

129. The PII that was publicized during the Data Breach was highly sensitive and highly private, as it included sensitive health information.

130. Forefront knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and class members' position would consider its actions highly offensive and its publication of sensitive PII as highly offensive, given the sensitive, private, and confidential nature of such information.

131. The private PII disclosed by Forefront without authorization is not of concern to the public.

132. As a proximate result of such unauthorized disclosures, Plaintiff's and class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Forefront's conduct amounted to a substantial and highly offensive invasion of Plaintiff's and class members' protected privacy interests.

133. Plaintiff seeks injunctive relief, restitution, and all other damages available under this Count.

## COUNT V
## UNJUST ENRICHMENT
## (PLEADING IN THE ALTERNATIVE)

134. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

135. This claim is pleaded in the alternative to Plaintiff's claim for breach of implied contract.

136. Plaintiff and class members conferred a monetary benefit upon Forefront in the form of monies paid for dermatology and related health services.

137. Forefront appreciated or had knowledge of the benefits conferred upon it by Plaintiff and class members. Forefront also benefited from the receipt of Plaintiff's and class members' PII.

138. The monies paid by Plaintiff and class members to Forefront were supposed to be used by Forefront, in part, to pay for adequate data security infrastructure, practices, and procedures.

139. As a result of Forefront's conduct, Plaintiff and class members suffered actual damages. For example, and not by way of limitation, Plaintiff and class members suffered benefit of bargain damages in an amount equal to the difference in value between what they paid for, i.e., health services if they had been protected by adequate data security, and what was actually received, i.e., services without adequate data security.

140. Forefront accepted and has retained these monetary benefits, and such acceptance and continued retention is inequitable and unjust. Because Forefront failed to implement (or adequately implement) data security practices that were otherwise mandated by the laws and industry standards alleged herein, principles of equity and good conscience militate against Forefront retaining the money belonging to Plaintiff and class members.

141. Forefront should be compelled to disgorge into a common fund for the benefit of Plaintiff and class members all unlawful or inequitable proceeds that Forefront received as a result of its conduct and the Data Breach alleged herein.

**COUNT VI**
**DECLARATORY RELIEF**
**28 U.S.C. § 2201**

142. Plaintiff realleges and incorporates all previous allegations as though fully set forth

herein.

143. An actual controversy has arisen and exists between Plaintiff and class members, on the one hand, and Forefront, on the other hand, concerning the Data Breach and Forefront's failure to protect Plaintiff's and class members' PII, including with respect to the issue of whether Forefront took adequate measures to protect that information. Plaintiff and class members are entitled to judicial determination as to whether Forefront has performed and is adhering to all data privacy obligations as required by law or otherwise to protect Plaintiff's and class members PII from unauthorized access, disclosure, and use.

144. A judicial determination of the rights and responsibilities of the parties regarding Forefront's privacy policies and whether it failed to adequately protect PII is necessary and appropriate to determine with certainty the rights of Plaintiff and the class members, and so that there is clarity between the parties as to Forefront's data security obligations with respect to PII going forward, in view of the ongoing relationships between the parties.

## PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the class members, by and through undersigned counsel, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as class representative and undersigned counsel as class counsel;

B. Award Plaintiff and class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining Forefront from continuing the unlawful practices as set forth above;

D. Award Plaintiff and class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and class members such other favorable relief as allowable under law or at equity.

**JURY TRIAL DEMANDED**

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

Dated: July 29, 2021

Respectfully submitted,

s/ John D. Blythin
Shpetim Ademi (SBN 1026973)
John D. Blythin (SBN 1046105)
**ADEMI LLP**
3620 East Layton Avenue
Cudahy, WI 53110
(414) 482-8000
(414) 482-8001 (fax)
sademi@ademilaw.com
jblythin@ademilaw.com

TINA WOLFSON*
*twolfson@ahdootwolfson.com*
ROBERT AHDOOT*
*rahdoot@ahdootwolfson.com*
THEODORE MAYA*
*tmaya@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH*
*aferich@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

**pro hac vice* to be filed

*Attorneys for Plaintiff and the Proposed Classes*

JS 44 (Rev. 10/20)

# 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.)*

Place an "X" in the appropriate box (required): ☒ Green Bay Division ☐ Milwaukee Division

**I. (a) PLAINTIFFS**
Lynn Anderson

**(b)** County of Residence of First Listed Plaintiff _____
*(EXCEPT IN U.S. PLAINTIFF CASES)*

**(c)** Attorneys *(Firm Name, Address, and Telephone Number)*
Ademi LLP, 3620 E. Layton Ave., Cudahy, WI 53110
414-482-8000

**DEFENDANTS**
Forefront Dermatology, S.C. and Forefront Management, LLC

County of Residence of First Listed Defendant _____
*(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)*

Click here for: Nature of Suit Code Descriptions.

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

**TORTS**

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

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

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

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

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

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

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

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

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

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

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

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

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

**PRISONER PETITIONS**

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

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

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

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

## VI. CAUSE OF ACTION

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

Brief description of cause:
Negligence, negligence per se, breach of implied contract, invasion of privacy, unjust enrichment, declaratory relief

## 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 _____ DOCKET NUMBER _____

DATE
07/29/2021

SIGNATURE OF ATTORNEY OF RECORD
s/ John D. Blythin

**FOR OFFICE USE ONLY**

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE



Print Save As... Reset

# 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 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.

# UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

LYNN ANDERSON

*Plaintiff(s)*

v.

FOREFRONT DERMATOLOGY, S.C. and FOREFRONT MANAGEMENT, LLC

*Defendant(s)*

Civil Action No. 21-cv-

## SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* FOREFRONT DERMATOLOGY, S.C.
c/o C T CORPORATION SYSTEM
301 S. BEDFORD ST., SUITE 1
MADISON, WI 53703

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you receive 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 the plaintiff's attorney, whose name and address are:

John D. Blythin
Ademi LLP
3620 E. Layton Ave.
Cudahy, WI 53110

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.

*GINA M. COLLETTI, CLERK OF COURT*

Date: _____

_____
*Signature of Clerk or Deputy Clerk*

Civil Action No. 21-cv-

**PROOF OF SERVICE**

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

This summons and the attached complaint for *(name of individual and title, if any):* _____

were received by me on *(date)* _____.

☐ I personally served the summons and the attached complaint on the individual at *(place):* _____

_____ on *(date)* _____ ; or

☐ I left the summons and the attached complaint 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 and the attached complaint 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.:



Print Save As... Reset

# UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

LYNN ANDERSON

*Plaintiff(s)*

v.

FOREFRONT DERMATOLOGY, S.C. and FOREFRONT MANAGEMENT, LLC

*Defendant(s)*

Civil Action No. 21-cv-

## SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* FOREFRONT MANAGEMENT, LLC
c/o C T CORPORATION SYSTEM
301 S. BEDFORD ST., SUITE 1
MADISON, WI 53703

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you receive 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 the plaintiff's attorney, whose name and address are:

John D. Blythin
Ademi LLP
3620 E. Layton Ave.
Cudahy, WI 53110

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.

*GINA M. COLLETTI, CLERK OF COURT*

Date: _____

_____
*Signature of Clerk or Deputy Clerk*

Civil Action No. 21-cv-

**PROOF OF SERVICE**

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

This summons and the attached complaint for *(name of individual and title, if any):* _____

were received by me on *(date)* _____.

☐ I personally served the summons and the attached complaint on the individual at *(place):* _____

_____ on *(date)* _____ ; or

☐ I left the summons and the attached complaint 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 and the attached complaint 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.:



Print Save As... Reset

# ClassAction.org