IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

JAMES JINDRA, on behalf of himself and all others similarly situated, *Plaintiff*, v. **OHIO MEDICAL ALLIANCE LLC d/b/a OHIO MARIJUANA CARD,** *Defendant*.	No. 1:25-cv-01837 **CLASS ACTION COMPLAINT** DEMAND FOR A JURY TRIAL

Plaintiff James Jindra, on behalf of himself and all others similarly situated, alleges the following against Defendant Ohio Medical Alliance LLC, doing business as Ohio Marijuana Card ("Defendant"), upon personal knowledge as to his own acts, and based upon his investigation, his counsel's investigation, and information and belief as to all other matters.

INTRODUCTION

1. On or around July 14, 2025,[1] cybersecurity researcher Jeremiah Fowler discovered an unencrypted and non-password-protected database containing 957,434 records with a total size of 323 gigabytes.[2] These records included high-resolution images of driver's licenses or identification documents that contained names, physical addresses, dates of birth, and license numbers; first and last names; intake forms; medical records; release forms; physician certification forms with Social Security numbers; mental health evaluations; diagnoses; and identification

[1] Lily Hay Newman & Matt Burgess, *Highly Sensitive Medical Cannabis Patient Data Exposed by Unsecured Database*, Wired (Aug. 19, 2025), https://www.wired.com/story/highly-sensitive-medical-cannabis-patient-data-exposed-by-unsecured-database/ (last accessed Aug. 28, 2025).

[2] Jeremiah Fowler, *Nearly a Million Records, Including Identification Documents and Health Data Exposed in Medical Marijuana Data Breach*, Website Planet, https://www.websiteplanet.com/news/ohio-medical-alliance-breach-report/ (last accessed Aug. 28, 2025).

documents from multiple states.[3] There was also a comma-separated values (CSV) file that contained internal communications, notes about clients, appointments, status, or personal situations, and an estimated 210,620 email addresses of clients and internal employees or business partners.[4]

2. The records are believed to belong to Defendant Ohio Medical Alliance d/b/a Ohio Marijuana Card.[5] Fowler immediately informed Defendant upon discovering the database, but it is unknown how long the records were exposed prior to Fowler's discovery.[6]

3. Defendant provides telehealth and in-person services to patients seeking medical evaluations for state medical marijuana cards in Ohio, Arkansas, Kentucky, Louisiana, Virginia, and West Virginia.[7]

4. In the course of providing these services, Defendant received PII and PHI from numerous individuals, including Plaintiff. In turn, Defendant came into the possession of, and maintains extensive files containing PII and PHI of these individuals, and owes these individuals an affirmative duty to adequately protect and safeguard this private information against theft and misuse. Despite such duties created by statute, regulation, and common law, at all relevant times, Defendant utilized deficient data security practices, thereby allowing sensitive and private data to fall into the hands of strangers.

5. This class action arises out of Defendant's failure to adequately secure the personally identifiable information ("PII") and protected health information ("PHI") (collectively,

---

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *About Ohio Marijuana Card*, https://www.ohiomarijuanacard.com/about-ohio-marijuana-card (last accessed Aug. 28, 2025).

the "Private Information") of individuals whose information was provided to Defendant in connection with Defendant's services (the "Cybersecurity Incident").

6. But for Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect these individuals' PII and PHI, the Cybersecurity Incident would not have occurred. The Cybersecurity Incident also results from Defendant's failure to implement reasonable and industry-standard data security practices necessary to protect its systems from a foreseeable cyberattack.

7. Defendant is well-aware that it is at high risk of attempted cyberattack due to the high value of the sensitive data. The cannabis industry is especially vulnerable because it is still emerging, and businesses are still figuring out best practices.[8]

8. Defendant is also aware of the sensitivity involved with marijuana, which remains illegal under federal law. Many individuals do not want to disclose the health conditions underlying their medical marijuana use and/or the fact that they use medical marijuana. Medical marijuana use remains highly stigmatized among employers, healthcare providers, and child welfare professionals.

9. Defendant claimed on its website that "The privacy of our patients is a top priority of ours, so we make sure all medical marijuana patient information is kept confidential."[9] This turned out not to be the case.

10. Despite Defendant's awareness of both the value and sensitivity of the data it safeguarded and serious risk presented by insufficient security practices, Defendant did not take

[8] *A Guide to Cannabis Cyber Security*, cure8 Blog (June 12, 2024), https://cure8.tech/a-guide-to-cannabis-cyber-security/ (last accessed Aug. 28, 2025).

[9] Frequently Asked Questions, https://www.ohiomarijuanacard.com/marijuana-faqs (last accessed Aug. 28, 2025).

sufficient steps to ensure that its systems were secure. Defendant knew or should have known about the risk to the data it stored and processed, and the critical importance of adequate security measures in the face of increasing threats.

11. Through this wrongful conduct, Plaintiff and Class Members are now at a significantly increased and impending risk of fraud, identity theft, and similar forms of criminal mischief—risks which may last the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes. Moreover, Plaintiff and Class Members have lost the inherent value of their private data.

12. By aggregating information obtained from the unsecured databases or other methods, criminals can assemble a full dossier of private information on an individual to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims' names and other personal information to open new financial accounts, incur credit charges, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it. Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security. Likewise, the exfiltration of protected health information puts Plaintiff and the Class Members at a present and continuing risk of medical identity theft, which poses an even more critical threat to victims because such fraud could lead to loss of access to necessary healthcare through misuse of paid-for insurance benefits or by incurring substantial medical debt.

13. Moreover, Defendant's failure to notify Plaintiff and Class Members about the Cybersecurity Incident harmed Plaintiff and made it more difficult for Plaintiff to take swift action to respond to the Cybersecurity Incident.

14. Plaintiff and Class Members have been harmed because they are at immediate risk of having their personal information used against them. Plaintiff does not know if his data has been sold, transferred, replicated, or irrevocably disseminated and exposed. Plaintiff has suffered harm in the loss of the value of his data which cannot be easily recovered, if ever.

15. Plaintiff, individually and on behalf of a nationwide class, alleges claims of (1) Negligence, (2) Negligence *Per Se*, (3) Breach of Implied Contract, and (4) Unjust Enrichment. Plaintiff also seeks declaratory and injunctive relief. Plaintiff asks the Court to compel Defendant to adopt reasonable information security practices to secure the sensitive PII and PHI that Defendant collects and stores in its databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiff

16. Plaintiff James Jindra is a resident and citizen of Columbus Heights, Ohio.

Defendant

17. Defendant Ohio Medical Alliance, LLC, is a limited liability company formed under the laws of Ohio doing business as Ohio Marijuana Card, with its headquarters at 4500 Rockside Road, Independence, OH 44131.

JURISDICTION AND VENUE

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

interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has personal jurisdiction over Defendant through its business operations in this District, the specific nature of which occurs in this District. Defendant's principal place of business is in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendant is also based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members from and/or in this District.

FACTUAL ALLEGATIONS

I. Background

21. Medical marijuana was legalized in Ohio on September 8, 2016.[10]

22. The Ohio State Board of Pharmacy issues patient identification cards, also known as medical marijuana cards, after a physician certifies an individual as a medical marijuana patient.[11]

23. There are currently 26 qualifying medical conditions for medical marijuana in Ohio, including Crohn's disease, Hepatitis C, cancer, and post-traumatic stress disorder.[12]

[10] State Medical Bd. of Ohio, *Medical Marijuana*, https://med.ohio.gov/for-the-public/medical-marijuana/ohio-medical-marijuana-control-program (last accessed Aug. 28, 2025).

[11] *How to Get an Ohio Marijuana Card*, https://www.ohiomarijuanacard.com/qualify-for-ohio-marijuana-card (last accessed Aug. 28, 2025).

[12] State Medical Bd. of Ohio, *Covered Conditions*, https://med.ohio.gov/for-the-public/medical-marijuana/covered-conditions (last accessed Aug. 28, 2025).

24. Defendant facilitates the process of obtaining medical marijuana cards. To book an appointment with a physician through Defendant, a patient must complete an intake form, make payment, submit documentation relevant to the qualifying condition, and identification for the state patient registry.[13] Patients such as Plaintiff and Class Members have entrusted Defendant with highly sensitive personal information. In the ordinary course of receiving services from Defendant, Plaintiff and Class Members were required to provide their Private Information to Defendant.

25. Defendant claims to have served 340,000 patients since its founding.[14] Defendant also has locations in Arkansas, Kentucky, Louisiana, Virginia, and West Virginia.

26. Defendant's Frequently Asked Questions includes the question "Is My Personal Information Kept Private?"[15] Defendant's answer to the question is: "The privacy of our patients is a top priority of ours, so we make sure all medical marijuana patient information is kept confidential in our HIPAA compliant file storage system."[16]

27. Defendant further guarantees that only "your recommending physician, dispensaries, and Ohio Board of Pharmacy will have access to" the Ohio Board of Pharmacy's Patient Registry.[17]

28. Defendant's Privacy Policy claims, "Ohio Medical Alliance uses reasonable and appropriate security measures to safeguard the information that has been collected from you via

[13] *Frequently Asked Questions*, https://www.ohiomarijuanacard.com/marijuana-faqs (last accessed Aug. 28, 2025).

[14] https://www.ohiomarijuanacard.com (last accessed Aug. 28, 2025).

[15] *Most Frequently Asked Questions About Getting a Medical Marijuana Card in Ohio*, https://www.ohiomarijuanacard.com/frequently-asked-questions (last accessed Aug. 28, 2025).

[16] *Id.*

[17] *Id.*

the public or Secure Website Services. Among the measures that Ohio Medical Alliance has implemented for its websites are administrative, physical and technical safeguards."[18]

II. Defendant's Failure to Safeguard the PII/PHI of Plaintiff and the Class

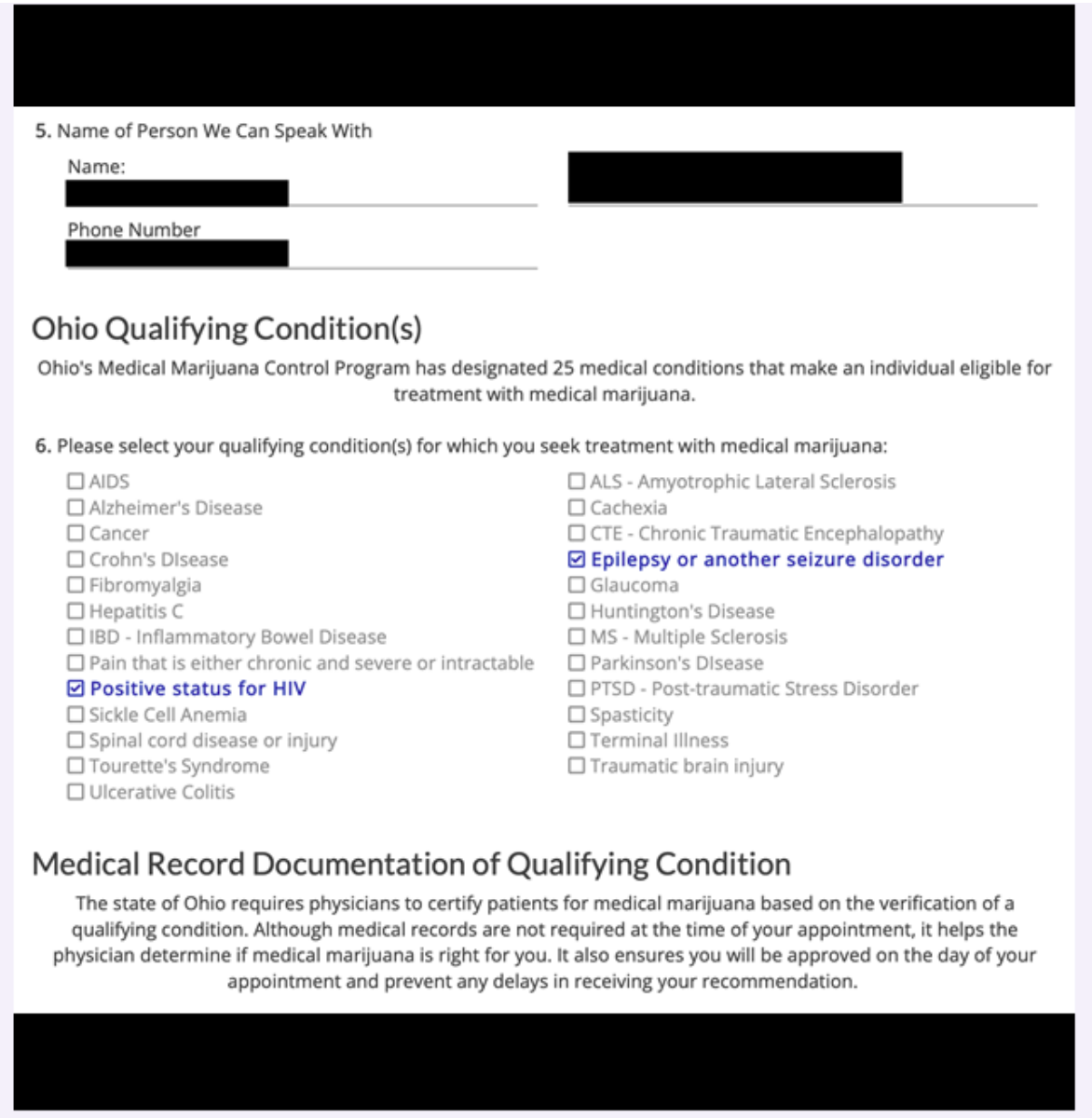
29. On or around July 14, 2025, cybersecurity researcher Jeremiah Fowler discovered an unencrypted and non-password-protected database containing 957,434 records with a total size of 323 gigabytes.[19] These records included high-resolution images of driver's licenses or identification documents that contained names, physical addresses, dates of birth, and license numbers.[20] A screenshot of these high-resolution images found by Fowler is below:

[18] *Ohio Medical Alliance's Privacy Policy and Terms & Conditions of Use*, https://www.ohiomarijuanacard.com/terms-and-privacy (last accessed Aug. 28, 2025).

[19] Jeremiah Fowler, *Nearly a Million Records, Including Identification Documents and Health Data Exposed in Medical Marijuana Data Breach*, Website Planet, https://www.websiteplanet.com/news/ohio-medical-alliance-breach-report/ (last accessed Aug. 28, 2025).

[20] *Id.*

30. The records also included first and last names; intake forms; medical records; release forms; physician certification forms with Social Security numbers; mental health evaluations; diagnoses; and identification documents from multiple states.[21] A screenshot of a medical record is below:



5. Name of Person We Can Speak With

Name: [redacted]

Phone Number [redacted]

Ohio Qualifying Condition(s)

Ohio's Medical Marijuana Control Program has designated 25 medical conditions that make an individual eligible for treatment with medical marijuana.

6. Please select your qualifying condition(s) for which you seek treatment with medical marijuana:

- ☐ AIDS
- ☐ Alzheimer's Disease
- ☐ Cancer
- ☐ Crohn's Disease
- ☐ Fibromyalgia
- ☐ Hepatitis C
- ☐ IBD - Inflammatory Bowel Disease
- ☐ Pain that is either chronic and severe or intractable
- ☑ **Positive status for HIV**
- ☐ Sickle Cell Anemia
- ☐ Spinal cord disease or injury
- ☐ Tourette's Syndrome
- ☐ Ulcerative Colitis
- ☐ ALS - Amyotrophic Lateral Sclerosis
- ☐ Cachexia
- ☐ CTE - Chronic Traumatic Encephalopathy
- ☑ **Epilepsy or another seizure disorder**
- ☐ Glaucoma
- ☐ Huntington's Disease
- ☐ MS - Multiple Sclerosis
- ☐ Parkinson's Disease
- ☐ PTSD - Post-traumatic Stress Disorder
- ☐ Spasticity
- ☐ Terminal Illness
- ☐ Traumatic brain injury

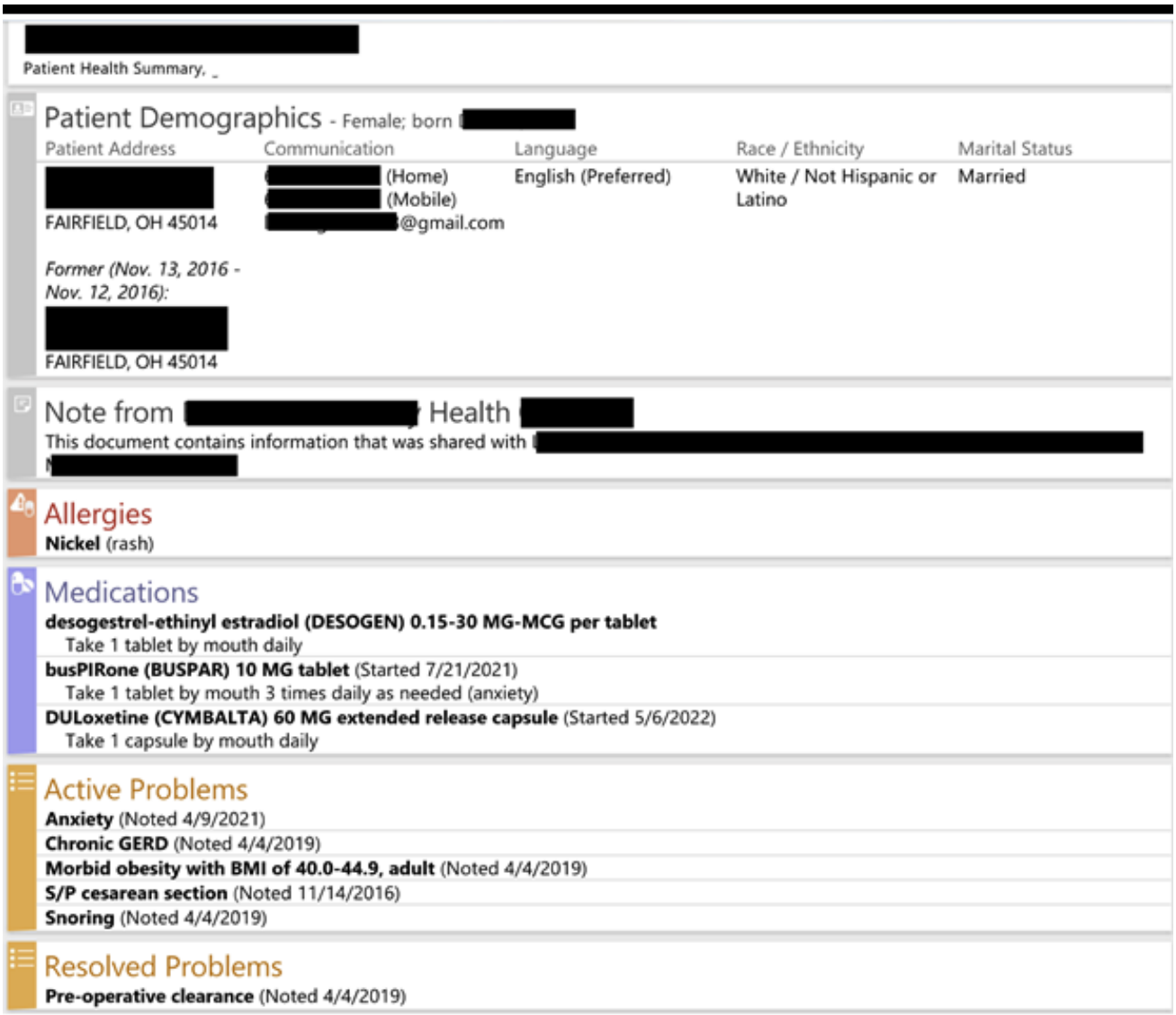
Medical Record Documentation of Qualifying Condition

The state of Ohio requires physicians to certify patients for medical marijuana based on the verification of a qualifying condition. Although medical records are not required at the time of your appointment, it helps the physician determine if medical marijuana is right for you. It also ensures you will be approved on the day of your appointment and prevent any delays in receiving your recommendation.

[redacted]

[21] *Id.*

31. The exposed health records revealed significant details about the patients, such as their non-medical-marijuana related diagnoses, allergies, and prior medical history, as shown in the screenshot below:


[redacted]
Patient Health Summary, _

Patient Demographics - Female; born [redacted]

Patient Address	Communication	Language	Race / Ethnicity	Marital Status
[redacted] FAIRFIELD, OH 45014	[redacted] (Home) [redacted] (Mobile) [redacted]@gmail.com	English (Preferred)	White / Not Hispanic or Latino	Married

Former (Nov. 13, 2016 - Nov. 12, 2016):
[redacted]
FAIRFIELD, OH 45014

Note from [redacted] Health [redacted]
This document contains information that was shared with [redacted]

Allergies
Nickel (rash)

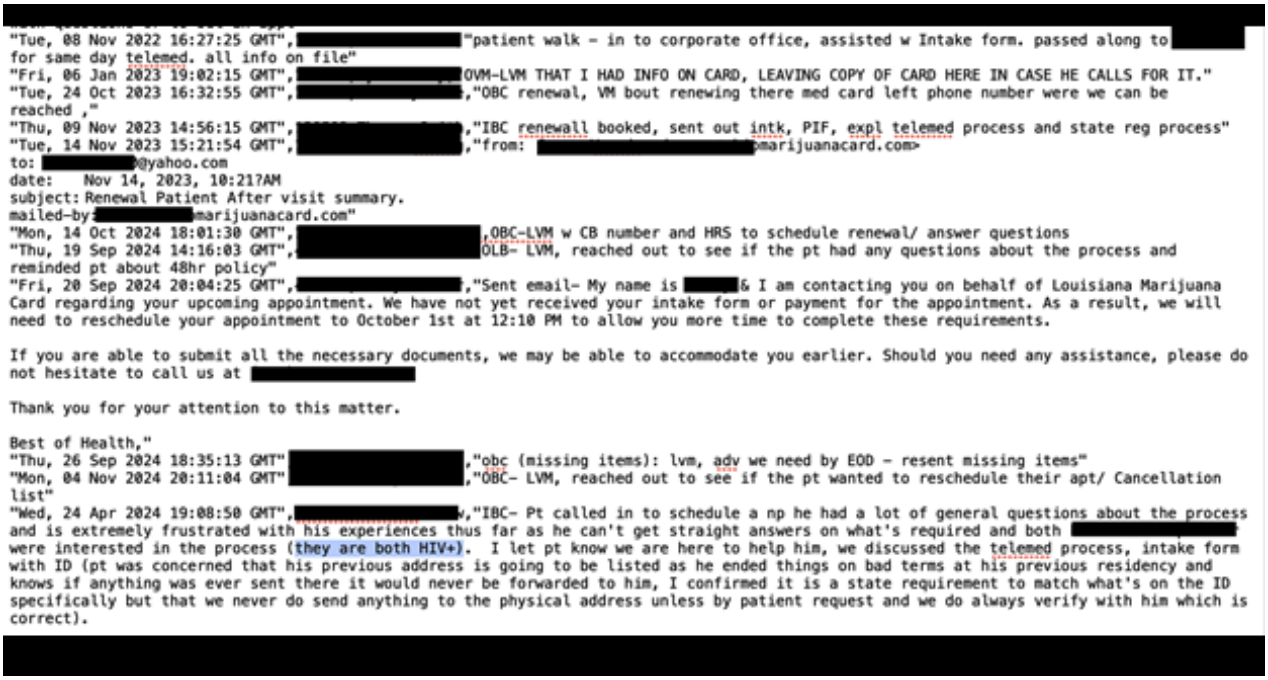
Medications
desogestrel-ethinyl estradiol (DESOGEN) 0.15-30 MG-MCG per tablet
Take 1 tablet by mouth daily
busPIRone (BUSPAR) 10 MG tablet (Started 7/21/2021)
Take 1 tablet by mouth 3 times daily as needed (anxiety)
DULoxetine (CYMBALTA) 60 MG extended release capsule (Started 5/6/2022)
Take 1 capsule by mouth daily

Active Problems
Anxiety (Noted 4/9/2021)
Chronic GERD (Noted 4/4/2019)
Morbid obesity with BMI of 40.0-44.9, adult (Noted 4/4/2019)
S/P cesarean section (Noted 11/14/2016)
Snoring (Noted 4/4/2019)

Resolved Problems
Pre-operative clearance (Noted 4/4/2019)

32. There was also a comma-separated values (CSV) file that contained internal communications, notes about clients, appointments, status, or personal situations, and an estimated

210,620 email addresses of clients and internal employees or business partners.[22] This file contains detailed comments about the patients, as shown in the screenshot of the CSV file below:



33. Defendant still has not publicly disclosed the Cybersecurity Incident, its cause, or its duration.

34. Without these details, Plaintiff's and Class Members' ability to mitigate harms resulting from the Cybersecurity Incident is severely diminished.

35. Defendant offers no substantive steps to help victims like Plaintiff, which is woefully inadequate considering the lifelong increased risk of fraud and identity theft that Plaintiff and Class Members now face as a result of the Cybersecurity Incident.

III. The Healthcare Sector Is Increasingly Susceptible to Data Breaches, Giving Defendant Ample Notice That It Was a Likely Cyberattack Target

36. At all relevant times, Defendant knew, or should have known, that the PII and PHI it was entrusted with was a target for malicious actors. Defendant knew this given the unique type

[22] *Id.*

and the significant volume of data on its networks, servers, and systems, comprising individuals' detailed and confidential personal information and, thus, the significant number of individuals who the exposure of the unencrypted data would harm.

37. As custodian of Plaintiff's and Class Members' PII and PHI, Defendant knew or should have known the importance of protecting their PII and PHI, and of the foreseeable consequences and harms to such persons if their data was exposed.

38. Defendant was on notice that the FBI has been long concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[23]

39. In January 2023, HHS created a presentation specifically for healthcare providers and IT departments, warning entities like Defendant of the severe threats posed by cybercriminal groups.[24]

40. Defendant's security obligations were especially important due to the substantial increase of cyberattacks and data breaches in recent years, particularly those targeting healthcare businesses and other organizations like Defendant, which store and maintain large volumes of PII and PHI. These largescale cyberattacks are increasingly common and well-publicized. Through the end of November 2023, 640 largescale cyberattacks had targeted hospitals, health systems, and

[23] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[24] *See Royal & BlackCat Ransomware: The Threat to the Health Sector*, https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf (last accessed June 24, 2025).

healthcare records in 2023, affecting more than 115 million people—making 2023 the "worst-ever year for breached healthcare records."[25]

41. Furthermore, the cannabis industry has also faced significant security risks. In 2020, Aurora Cannabis experienced a cyberattack in which employees' credit card information, home addresses, banking details, and other government identification information was compromised.[26]

42. Between October 10, and November 10, 2024, California-based cannabis brand Stiiizy experienced a ransomware attack, which it disclosed in January 2025.[27] The data breach impacted 380,000 individuals, whose compromised data included: names, addresses, dates of birth, driver license numbers, passport numbers, photographs, age details, medical cannabis cards, signatures on government ID cards, and transaction histories.[28]

43. Stiiizy is one of the largest cannabis retail store chains in California.[29]

44. An informal survey conducted in 2021 by MJBiz found that 59% of the marijuana companies surveyed had not taken any steps to prevent ransomware attacks.[30]

---

[25] *November 2023 Healthcare Data Breach Report*, The HIPAA Journal (Dec. 21, 2023), https://www.hipaajournal.com/november-2023-healthcare-data-breach-report/.

[26] *A Guide to Cannabis Cyber Security*, cure8 Blog (June 12, 2024), https://cure8.tech/a-guide-to-cannabis-cyber-security/ (last accessed Aug. 28, 2025).

[27] Ionut Arghire, *380,000 Impacted by Data Breach at Cannabis Retailer Stiiizy*, SecurityWeek (Jan. 16, 2025), https://www.securityweek.com/380000-impacted-by-data-breach-at-cannabis-retailer-stiiizy/ (last accessed Aug. 28, 2025).

[28] *Id.*

[29] *Id.*

[30] Margaret Jackson, *Cannabis companies considered ripe targets for ransomware attacks*, MJBiz Daily (Sept. 20, 2021), https://mjbizdaily.com/cannabis-companies-considered-ripe-targets-for-ransomware-attacks/ (last accessed Aug. 28, 2025).

45. Ransomware groups often post links to stolen data on a Data Leak Site ("DLS").[31] A DLS is a "website where the illicitly retrieved data of companies, that refuse to pay the ransom, are published."[32]

46. However, even if a ransomware group removes stolen data from its DLS when a ransom is paid, there is no guarantee that the data will be deleted.[33] The stolen Private Information is valuable, and can easily be sold to another threat actor, so there is little incentive to delete it.[34]

47. Ransomware groups can therefore monetize stolen Private Information and sell it on the dark web as part of a full identity profile.[35] Buyers can then use that information to conduct different types of identity theft or fraud, such as to file a fake tax return, to apply for a fraudulent mortgage or to open a bank account while impersonating the victim.[36]

48. Patient records, such as those left unprotected by Defendant, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail."[37] The record sets are then sold on Dark Web sites to other criminals and "allows an identity kit to be created, which can then be sold

---

[31] Steve Alder, *Majority of Ransomware Victims That Pay a Ransom Suffer a Second Attack*, The HIPAA Journal (Feb. 23, 2024), https://www.hipaajournal.com/majority-of-ransomware-victims-that-pay-a-ransom-suffer-a-second-attack/#:~:text=While%20ransomware%20groups%20usually%20remove,little%20incentive%20to%20delete%20it. (last accessed July 23, 2025).

[32] *Dedicated Leak Sites (DLS): Here's what you should know*, Group-IB, https://www.group-ib.com/resources/knowledge-hub/dedicated-leak-sites/ (last accessed April 3, 2025).

[33] Alder, *supra* note 27.

[34] *Id.*

[35] Anthony M. Freed, *Which Data Do Ransomware Attackers Target for Double Extortion?*, maliciouslife by cybereason, https://www.cybereason.com/blog/which-data-do-ransomware-attackers-target-for-double-extortion (last accessed July 3, 2025).

[36] *Id.*

[37] Steve Alder, *Editorial: Why Do Criminals Target Medical Records*, The HIPAA Journal (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last accessed Aug. 22, 2025).

for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[38]

49. With the surging number of such attacks targeting companies in the healthcare sector, Defendant knew or should have known that it was at high risk of cyberattack and should have taken additional and stronger precautions and preemptive measures.

50. The information compromised in the Cybersecurity Incident—including detailed medical information—is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here, however, the information compromised is much more difficult, if not impossible, for consumers to re-secure after being stolen because it goes to the core of their identity. An individual's medical history and assessments are permanent and are impossible to escape. The loss of all this medical data puts Plaintiff and Class Members at additional risk for potential medical fraud and medical identity theft.

51. Data disclosures involving medical records are not only incredibly costly, they can "also [be] more difficult to detect, taking almost twice as long as normal identity theft."[39] The FTC warns that a thief may use private medical information to, among other things, "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care"[40] and that this may have far reaching consequences for a victim's ability to access medical care and use insurance benefits.

---

[38] *Id.*

[39] Federal Trade Commission Consumer Information, *What to Know About Medical Identity Theft*, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 22, 2023).

[40] *Id.*

IV. Defendant Failed to Comply with FTC Guidelines

52. At all times relevant to this Complaint, Defendant knew or should have known the significance and necessity of safeguarding PII and PHI, and the foreseeable consequences of a data breach. Defendant knew or should have known that because it collected and maintained the PII and PHI for a significant number of patients, employees, and business partners, a significant number of patients, employees, and business partners would be harmed by a breach of its systems. Defendant further knew due to the nature of its business practices that the data it was entrusted with was highly valuable and contained private and sensitive information including medical information.

53. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding sensitive PII and emphasized the importance of adequate data security practices. The FTC also stresses that appropriately safeguarding PII held by businesses should be factored into all business-related decision making.

54. An FTC Publication titled "Protecting Personal Information: A Guide for Business" lays out fundamental data security principles and standard practices that businesses should implement to protect PII.[41] The guidelines highlight that businesses should (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems.

55. The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.

---

[41] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last accessed March 21, 2024).

56. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

57. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

58. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

59. Defendant knew or should have known of its obligation to implement appropriate measures to protect PII in its possession but failed to comply with the FTC's basic guidelines.

60. Defendant's failure to employ reasonable measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

61. Once Defendant became aware of the Cybersecurity Incident, it could have assisted victims in redressing harms or at least notified victims of the unauthorized exposure.

62. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of

time—months or even years—to use the PII obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the PII easier to use without detection. These identity thieves will also re-use stolen PII and PHI, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their PII and PHI.

63. Victims of data breaches are much more likely to become victims of identity fraud than those who have not. Victims who do experience identity theft resulting from cybersecurity incidents or data breaches often spend hundreds of hours fixing the damage caused by identity thieves.[42] Plaintiff and Class Members generally have spent considerable time and stress in attempting to mitigate the present and future harms caused by the breach. The U.S. Department of Justice's Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims "reported spending an average of about 7 hours clearing up the issues."[43]

64. The information compromised in the Cybersecurity Incident—including detailed medical information—is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here, however, the information compromised is much more difficult, if not impossible, for consumers to re-secure after being stolen because it goes to the core of their identity. An individual's medical history and assessments are permanent and are impossible to escape. The loss of all this medical data puts Plaintiff and

[42] Maryland Office of the Attorney General, *Identity Theft: Protect Yourself, Secure Your Future*, https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf (last accessed July 2, 2025).

[43] Erika Harrell, *Victims of Identity Theft, 2014*, U.S. Dep't of Justice, https://bjs.ojp.gov/content/pub/pdf/vit14.pdf. (last accessed July 2, 2025).

Class Members at additional risk for potential medical fraud and medical identity theft. This is particularly problematic for medical marijuana patients, who might have conditions that are stigmatized or that they wish to not disclose widely.

65. Data breaches and disclosures involving medical records are not only incredibly costly, they can "also [be] more difficult to detect, taking almost twice as long as normal identity theft."[44] The FTC warns that a thief may use private medical information to, among other things, "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care"[45] and that this may have far reaching consequences for a victim's ability to access medical care and use insurance benefits.

V. Defendant Failed to Comply with Industry Standards

66. Security standards for businesses storing PII and PHI commonly include, but are not limited to:

a) Maintaining a secure firewall

b) Monitoring for suspicious or unusual traffic on the website

c) Looking for trends in user activity including for unknown or suspicious users

d) Looking at server requests for PII

e) Looking for server requests from VPNs and Tor exit nodes

f) Requiring Multi-factor authentication before permitting new IP addresses to access user accounts and PII

[44] Federal Trade Commission Consumer Information, *What to Know About Medical Identity Theft*, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Nov. 22, 2023).

[45] *Id.*

g) Structuring a system including design and control to limit user access as necessary, including a user's access to the account data and PII of other users.

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

68. Defendant failed to meet minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR- DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM- 06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIC CSC), which are all established standards in reasonable cybersecurity readiness.

69. These frameworks are existing and applicable healthcare industry standards which Defendant failed to comply with.

VI. Defendant Failed to Comply with HIPAA Guidelines

70. HIPAA requires covered entities such as Defendant to protect against reasonably foreseeable threats to the security of sensitive patient health information.

71. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

72. Title II of HIPAA contains the Administrative Simplification provisions, which require that the Department of Health and Human Services ("HHS") create rules to streamline standards for handling PII like the data that was not adequately safeguarded by Defendant.

73. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI is properly maintained.[46]

74. The Cybersecurity Incident itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's safety failures include, but are not limited to:

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

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

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

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

e) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or

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

software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

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

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

VII. Plaintiff's and Class Members' Experiences

75. Plaintiff used Defendant's services in 2021 or 2022.

76. Plaintiff provided Defendant with his most sensitive medical and personal information and cannot be sure how much of it was exfiltrated.

77. Around six months to a year ago, Plaintiff was subscribed to tens or hundreds of email services all in the same morning. He did not voluntarily or intentionally subscribe to any of these email services.

78. Plaintiff suffered an actual injury in the form of damages and diminution in the value of his Private Information—a form of tangible property that Plaintiff entrusted to Defendant, which was compromised in and because of Defendant's failure to protect his data.

79. Plaintiff has suffered imminent and impending injury arising from the exacerbated risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

80. Plaintiff has a continuing interest in ensuring that his Private Information, which upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

VIII. Defendant Breached its Obligations to Plaintiff and the Class

81. Defendant fails to offer any compensation to victims of the Cybersecurity Incident, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiff's and Class Members' Private Information, out-of-pocket costs, and the time taken by Plaintiff and Class Members to mitigate their injuries.

82. Plaintiff and Class Members have been damaged by the severe disruption to their lives as a direct and foreseeable consequence of the Cybersecurity Incident.

83. Plaintiff and Class Members were damaged since their Private Information is being sold or potentially for sale by cybercriminals in the years to come.

84. As a direct and proximate consequence of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, actual, and substantial risk of harm from fraud and identity theft.

85. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Cybersecurity Incident.

86. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Cybersecurity Incident. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Cybersecurity Incident.

87. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

88. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was exposed as a result of the Cybersecurity Incident. Numerous courts have recognized the propriety of loss of value damages in related cases.

89. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.[47] The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to "pay an average of $13,500 to resolve the crime."[48]

90. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Cybersecurity Incident and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

---

[47] Federal Trade Commission, *Medical Identity Theft: FAQs for Health Care Providers and Health Plans*, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last accessed Jan. 8, 2024).

[48] Justin Klawans, *What is medical identity theft and how can you avoid it?*, The Week (Aug. 2, 2023), https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid (last accessed July 23, 2025).

91. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Cybersecurity Incident relating to:

a) Finding fraudulent charges;

b) Cancelling and reissuing credit and debit cards;

c) Purchasing credit monitoring and identity theft prevention;

d) Monitoring their medical records for fraudulent charges and data;

e) Addressing their inability to withdraw funds linked to compromised accounts;

f) Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g) Placing "freezes" and "alerts" with credit reporting agencies;

h) Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i) Contacting financial institutions and closing or modifying financial accounts;

j) Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k) Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l) Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

92. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial

information as well as health information is not accessible online and that access to such data is password protected.

93. Defendant's failure to report the Cybersecurity Incident caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early notification helps a victim mitigate their injuries, and conversely, delayed notification causes more harm and increases the risk of identity theft. It is unknown how long Plaintiff's and Class Members' Private Information was exposed. Defendant has still not informed affected individuals that their Private Information was exposed in the first place. This violates HIPAA and other notification requirements and increased injuries to Plaintiff and the Class.

CLASS ACTION ALLEGATIONS

94. Plaintiff brings this class action on behalf of himself and all other similarly situated individuals under Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3), on behalf of the following class (the "Class"):

> All persons in the United States whose Private Information was compromised as a result of Defendant's Cybersecurity Incident.

95. Excluded from the Class are governmental entities, Defendant, any entity in which Defendant have a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded from the Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

96. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements therein.

97. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. Upon information and belief, the Class consists of hundreds of thousands of

individuals. The precise number and identity of Class Members can be determined by information and records in the possession of Defendant.

98. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary among Class Members and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

a) Whether Defendant failed to take adequate and reasonable measures to ensure its website and data systems were protected;

b) Whether Defendant failed to take available steps to prevent and stop the Cybersecurity Incident from happening or mitigating the risk of a long-term breach;

c) Whether Defendant unreasonably delayed in notifying affected individuals of the harm they suffered once the suspicious activity was detected;

d) Whether Defendant owed a legal duty to Plaintiff and Class Members to protect their PII and PHI;

e) Whether Defendant breached any duty to protect the personal information of Plaintiff and Class Members by failing to exercise due care in protecting their PII and PHI;

f) Whether Defendant's conduct violated the statutes as set forth herein;

g) Whether Defendant took sufficient steps to secure Class Members' Private Information;

h) Whether Defendant was unjustly enriched;

i) Whether Plaintiff and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,

j) Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief or restitution.

99. **Typicality.** Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

100. **Adequacy of Representation.** Plaintiff is an adequate class representative because he is a Class Member, and his interests do not conflict with the Class's interests. Plaintiff retained counsel who are competent and experienced in class action and data breach litigation. Plaintiff and his counsel intend to prosecute this action vigorously for the Class's benefit.

101. **Predominance and Superiority.** The Class can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Class Member's claim is impracticable. Even if each Class Member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

102. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1
Negligence
On behalf of Plaintiff and the Class

103. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

104. Plaintiff was required to provide PII and PHI as a precondition for receiving Defendant's medical marijuana services. Plaintiff and Class Members entrusted their PII and PHI to Defendant with the understanding that it would safeguard their PII and PHI.

105. Defendant had full knowledge of the sensitivity of the PII and PHI that it stored and the types of harm that Plaintiff and Class Members could and would suffer if that PII and PHI were wrongfully disclosed.

106. Defendant violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Defendant's information security controls sufficiently rigorously to ensure that PII and PHI in its possession was adequately secured by, for example, encrypting sensitive personal information, installing effective intrusion detection systems and monitoring mechanisms, using

access controls to limit access to sensitive data, regularly testing for security weaknesses and failures, failing to notify patients of the specific breached data in a timely manner, and failing to remedy the continuing harm by unreasonably delaying notifying specific victims who were harmed.

107. Defendant's duty of care arose from, among other things,

a) The special relationship between Defendant, Plaintiff, and Class Members resulting from Plaintiff and Class Members entrusting Defendant with confidential PII/PHI;

b) Defendant's exclusive ability (and Class Members' inability) to ensure that its systems, website, and vendor services were sufficient to protect against the foreseeable risk that a data breach could occur;

c) HIPAA, which requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

d) Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures; and

e) Defendant's common law duties to adopt reasonable data security measures to protect customer and employee PII and PHI and to act under the same or similar circumstances as a reasonable and prudent person would act.

108. Plaintiff and Class Members were the foreseeable victims of Defendant's inadequate data security.

109. Defendant's conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's conduct included its failure to adequately mitigate harm through negligently failing to inform victims that their data was publicly exposed for an undetermined period of time.

110. Defendant knew or should have known of the inherent risks in collecting and storing massive amounts of PII and PHI and the importance of limiting disclosure of that PII and PHI.

111. Defendant, through its actions and inactions, breached its duty owed to Plaintiff and Class Members by failing to exercise reasonable care in safeguarding their PII and PHI while it was in its possession and control. Defendant breached its duty by, among other things, its failure to adopt reasonable data security practices and its failure to adopt reasonable security and notification practices, failure to monitor the security of its networks and systems, and allowing unauthorized access to Plaintiff's and Class Members' Private Information.

112. Defendant further breached its duties by failing to provide any notice of to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm and Plaintiff's and Class Members' injuries-in-fact.

113. Defendant inadequately safeguarded PII and PHI in breach of standard industry rules, regulations, and best practices.

114. There is a temporal and close causal connection between Defendant's failure to implement adequate data security measures and notification practices, the unauthorized disclosure, and the harms suffered by Plaintiff and Class Members.

115. As a result of Defendant's failure to 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.

116. As a direct and traceable result of Defendant's negligence, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary damages, increased risk of future harm, 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; 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, overpayment for the services and products that were received without adequate data security; and embarrassment, humiliation, and emotional distress.

117. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

118. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 2
Negligence *Per Se*
On behalf of Plaintiff and the Class

119. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

120. Section 5 of the FTC Act, 15 U.S.C. § 45 prohibits, "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information.

121. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with industry standards.

122. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems. Plaintiff was required to provide PII and PHI to Defendant. Plaintiff and Class Members entrusted their PII and PHI to Defendant with the understanding that Defendant would safeguard their PII and PHI.

123. Class Members are within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

124. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

125. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* 45 C.F.R. § 164.304 (defining "encryption").

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

127. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

128. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that

it failed to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

129. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Count 3
Breach of Implied Contract
On behalf of Plaintiff and the Class

130. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

131. Plaintiff and Class Members entered into an implied contract with Defendant when they paid Defendant, and entrusted Defendant with their PII and PHI as a precondition for receiving medical marijuana services.

132. Pursuant to these contracts, Plaintiff provided Defendant with his Private Information. In exchange, Defendant agreed to: (1) use such Private Information for business purposes only, (2) retain Private Information only under conditions that kept such information secure and confidential, (3) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' Private Information; and (4) protect Plaintiff's and Class Members' Private Information in compliance with federal and state laws and regulations, industry standards, and Defendant's representations regarding its security and privacy practices.

133. As part of these transactions, Defendant agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify them if their PII or PHI was breached or compromised.

134. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with the legal requirements, industry standards, and Defendant's own representations. Plaintiff and Class Members believed that Defendant would use part of the monies paid to Defendant under the implied contracts or the monies obtained from the benefits derived from the PII and PHI they provided to fund proper and reasonable data security practices.

135. Implicit in the agreement between Defendant, Plaintiff, and Class Members was the obligation that both parties would maintain information confidentially and securely.

136. These exchanges constituted an agreement and meeting of the minds between the parties.

137. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have provided and entrusted their PII and PHI to Defendant in the absence of the implied contract or implied terms between them and Defendant. The safeguarding of the PII and PHI of Plaintiff and Class Members was critical to realize the intent of the parties.

138. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

139. Defendant breached its implied contracts with Plaintiff and Class Members to protect their PII and PHI when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) failed to comply with industry standards; (3) failed to comply with the legal obligations necessarily incorporated into these agreements; and; (4) failed to notify Plaintiff and Class Members that their data was exposed.

140. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at

trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Cybersecurity Incident; reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because Defendant negligently maintained their Private Information; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

141. As a direct and proximate result of the unauthorized disclosure, Plaintiff and Class Members are entitled to relief as set forth herein.

142. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 4
Unjust Enrichment
On behalf of Plaintiff and the Class

143. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

144. This count is brought in the alternative to Plaintiff's breach of contract claim.

145. Plaintiff and Class Members conferred a benefit on Defendant by providing Private Information to Defendant. Moreover, upon information and belief, Plaintiff alleges that payments

made by them to Defendant included payment for cybersecurity protection, and that those cybersecurity costs were passed on to Plaintiff and Class Members in the form of elevated prices charged by Defendant for its services. Plaintiff and Class Members did not receive such cybersecurity protection. Specifically, they provided Defendant with their PII and PHI. In exchange, Defendant should have provided adequate data security for Plaintiff and Class Members.

146. Upon information and belief, Defendant funds its data security measures and website from its general revenue, including payments made by Plaintiff and Class Members.

147. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security including the protection of the data from inadvertent disclosure to third parties. Defendant's website and its security and privacy measures are entirely under the sole control of Defendant.

148. Defendant, however, failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

149. Defendant would not be able to carry out an essential function of its regular business without the money and Private Information provided by its patients. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

150. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

151. Defendant knew that Plaintiff and Class Members conferred a benefit upon it, which Defendant accepted. Defendant profited from these transactions and used the Private

Information of Plaintiff and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the unauthorized Cybersecurity Incident.

152. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have provided their Private Information to Defendant.

153. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the breach, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and cheaper contractors and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

154. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

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

156. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injuries that include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy

and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Cybersecurity Incident reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendant's Cybersecurity Incident; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

157. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members were underpaid by Defendant.

158. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 5
Injunctive/Declaratory Relief
On behalf of Plaintiff and the Class

159. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described herein.

160. Defendant owes a duty of care to Plaintiff and Class Members, which required Defendant to adequately monitor and safeguard Plaintiff's and Class Members' PII and PHI.

161. Defendant and its officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII and PHI belonging to Plaintiff and Class Members.

162. An actual controversy has arisen in the wake of the Cybersecurity Incident regarding Plaintiff's and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further cybersecurity incidents or data breaches that compromise their PII and PHI. Plaintiff allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and PHI and the risk remains that further compromises of their private information will occur in the future.

163. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a) Defendant owes a legal duty to adequately secure the PII and PHI of Plaintiff and the Class within its care, custody, and control under the common law, HIPAA, and Section 5 of FTC Act;

b) Defendant breached its duty to Plaintiff and the Class by allowing the Cybersecurity Incident to occur;

c) Defendant's existing data monitoring measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII and PHI of Plaintiff and the Class within Defendant's custody, care, and control; and

d) Defendant's ongoing breaches of said duties continue to cause harm to Plaintiff and the Class.

164. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with healthcare industry standards to protect the PII and PHI of Plaintiff and the Class within its custody, care, and control, including the following:

a) Order Defendant to provide lifetime credit monitoring and identity theft insurance and protection services to Plaintiff and Class Members; and

b) Order that, to comply with Defendant's obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:

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

ii. Encrypting and anonymizing the existing PII and PHI within its servers, networks, and systems to the extent practicable, and purging all such information which is no longer reasonably necessary for Defendant to provide adequate medical services to its patients;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;

v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendant's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

165. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another data breach or cybersecurity incident occurs, Plaintiff and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiff and the Class for the serious risks of future harm.

166. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

167. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach or cybersecurity incident, thus preventing future injury to Plaintiff and the Class and other persons whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action and appoint Plaintiff and his counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII and PHI of Plaintiff and the Class by implementing improved security controls;

C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;

F. That the Court award to Plaintiff and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate; and

H. All such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial of all claims so triable herein.

Dated: September 3, 2025

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579)
Dylan J. Gould (0097954)
Spencer D. Campbell (0103001)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com
scampbell@msdlegal.com

Amber L. Schubert*
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: 415-788-4220
Fax: 415-788-0161
aschubert@sjk.law

Counsel for Plaintiff and the Proposed Class

*admission application forthcoming

JS 44 (Rev. 09/23)

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

James Jindra, on behalf of himself and all others similarly situated

(b) County of Residence of First Listed Plaintiff Cuyahoga County, Ohi
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Markovits, Stock & DeMarco, LLC, 119 East Court St, Ste 530, Cincinnati, Ohio 45202. Tel. (513) 651-3700

DEFENDANTS

OHIO MEDICAL ALLIANCE 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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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

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

VI. CAUSE OF ACTION

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

Brief description of cause:
Data breach class action.

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ Exceeding $5 million

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Barker; Barker, Calabrese, Brennan, Fleming DOCKET NUMBER 1:25-cv-1765, 779, 793, 799, 1802

DATE
September 3, 2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ Terence R. Coates

FOR OFFICE USE ONLY

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

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

I. Civil Categories: (Please check one category only).

1. ☑ General Civil
2. ☐ Administrative Review/Social Security
3. ☐ Habeas Corpus Death Penalty

*If under Title 28, §2255, name the SENTENCING JUDGE: _____

CASE NUMBER: _____

II. **RELATED OR REFILED CASES** See LR 3.1 which provides in pertinent part: "If an action is filed or removed to this Court and assigned to a District Judge after which it is discontinued, dismissed or remanded to a State court, and subsequently refiled, it shall be assigned to the same Judge who received the initial case assignment without regardfor the place of holding court in which the case was refiled. Counsel or a party without counsel shall be responsible for bringing such cases to the attention of the Court by responding to the questions included on the Civil Cover Sheet."

This action: ☐ is **RELATED** to another **PENDING** civil case ☐ is a **REFILED** case ☐ was **PREVIOUSLY REMANDED**

If applicable, please indicate on page 1 in section VIII, the name of the Judge and case number.

III. In accordance with Local Civil Rule **3.8**, actions involving counties in the Eastern Division shall be filed at any of the divisional offices therein. Actions involving counties in the Western Division shall be filed at the Toledo office. For the purpose of determining the proper division, and for statistical reasons, the following information is requested.

ANSWER ONE PARAGRAPH ONLY. ANSWER PARAGRAPHS 1 THRU 3 IN ORDER. UPON FINDING WHICH PARAGRAPH APPLIES TO YOUR CASE, ANSWER IT AND STOP.

(1) **Resident defendant**. If the defendant resides in a county within this district, please set forth the name of such county

COUNTY: Cuyahoga

Corporation **For the purpose of answering the above, a corporation is deemed to be a resident of that county in which it has its principal place of business in that district.**

(2) **Non-Resident defendant.** If no defendant is a resident of a county in this district, please set forth the county wherein the cause of action arose or the event complained of occurred.

COUNTY:

(3) **Other Cases**. If no defendant is a resident of this district, or if the defendant is a corporation not having a principle place of business within the district, and the cause of action arose or the event complained of occurred outside this district, please set forth the county of the plaintiff's residence.

COUNTY:

IV. The Counties in the Northern District of Ohio are divided into divisions as shown below. After the county is determined in Section **III**, please check the appropriate division.

EASTERN DIVISION

☐	**AKRON**	**(Counties: Carroll, Holmes, Portage, Stark, Summit, Tuscarawas and Wayne)**
☑	**CLEVELAND**	**(Counties: Ashland, Ashtabula, Crawford, Cuyahoga, Geauga, Lake, Lorain, Medina and Richland)**
☐	**YOUNGSTOWN**	**(Counties: Columbiana, Mahoning and Trumbull)**

WESTERN DIVISION

☐	**TOLEDO**	**(Counties: Allen, Auglaize, Defiance, Erie, Fulton, Hancock, Hardin, Henry, Huron, Lucas, Marion, Mercer, Ottawa, Paulding, Putnam, Sandusky, Seneca VanWert, Williams, Wood and Wyandot)**

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

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

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

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

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

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

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

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

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

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

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

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

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

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of Ohio

JAMES JINDRA, on behalf of himself and all others similarly situated,

Plaintiff(s)

v.

OHIO MEDICAL ALLIANCE LLC

Defendant(s)

Civil Action No. 1:25-cv-01837

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* OHIO MEDICAL ALLIANCE LLC
C/O REGISTERED AGENTS INC.
6545 MARKET AVENUE NORTH, SUITE 100
NORTH CANTON OH 44721

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Terence R. Coates, Esq.
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202

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

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 1:25-cv-01837

PROOF OF SERVICE

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

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

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

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

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

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

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

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

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: