

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS**

C.K., on behalf of himself and all others similarly
situated by his guardian, AMY KMIECIK,

Plaintiff,

v.

ANN & ROBERT H. LURIE CHILDREN'S
HOSPITAL OF CHICAGO;

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff C.K., (“Plaintiff”), on behalf of himself and all others similarly situated, by his guardian Amy Kmiecik, alleges the following Class Action Complaint (the “Action”) against the above-captioned Defendant, Ann & Robert H. Lurie Children’s Hospital of Chicago (“Defendant” or “Lurie Children’s”) upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of his counsel as follows:

I. INTRODUCTION

1. Lurie Children’s is a top-ranked children’s hospital and healthcare provider in Illinois with over 50 locations spread throughout Illinois and the surrounding states. Lurie Children’s is a sophisticated organization which brings in tens of millions of dollars annually in donations and has numerous corporate partners, including Ace Hardware.

2. In the course of serving patients, Lurie Children’s collects a significant amount of data - including patients’ personal identifiable information (“PII”) name, address, date of birth, dates of service, driver’s license, email address, telephone number, Social Security number, as well as health information including health claims information, health plan, health plan beneficiary number, medical condition or diagnosis, medical record number, medical treatment, and prescription information (the “PHI” or, collectively, the “PII”). This is the PII that was exposed for Plaintiff and the Class members.

3. When patients initially disclosed this PII to Defendant, they did so under the impression that it would be protected in a manner consistent with how valuable this subset of PII is.

4. However, on June 27, 2024, Defendant disclosed that the PII of over 791,784 current or former patients, including mostly children, has been compromised in connection with a

malicious cyberattack that occurred between January 26, 2024 and January 31, 2024 (the “Data Breach”).

5. On January 31, 2024, “to protect our systems and our ability to continue operations,” according to Lurie Children’s Notice of Data Breach (the “Notice”), “Lurie Children’s took certain systems offline.” This, while not admitted in the Notice, is a telltale sign of a ransomware attack which preceded the Data Breach. A ransomware attack is a type of cybersecurity intrusion whereby the cybercriminal deploys “ransomware” on a given entity’s computer system and data storage network. Ransomware is a software that works to “lock” access to a given computer system or data storage network until the entity pays a ransom, usually in untraceable cryptocurrency, in order to regain access. In this instance, Lurie Children’s admits on its website that it “did not pay a ransom” but does not state as much in its Notice or go as far in either document to state that it was the victim of a ransomware attack.

6. Then, as stated in the Notice, Lurie Children’s waited over five months until June 27, 2024 to inform its patients that their PII and PHI could be compromised as a result of the Data Breach. This critical passage of time is and was harmful to the victims of the Data Breach. As is the case with data breaches generally, every moment is precious in order to recover data and take necessary safety measures to insulate from the many harms that data breaches cause.

7. Due to this conduct, Plaintiff and Class members have been exposed to actual harm consistent with the litany of injuries that data breaches cause, including (a) loss of value of PII, (b) loss of time spent dealing with the Data Breach, (c) imminent threat of and actual theft of PII by cybercriminals, and (d) any other types of quantifiable harm that stem from the breach, including out-of-pocket losses and money spent on identity theft monitoring.

8. As such, Plaintiff, on behalf of himself and all other similarly situated, brings this Action to seek actual damages, punitive damages, restitution, statutory damages, injunctive relief, and a declaratory judgment, as well as any other relief this Court may deem just and proper, for Lurie Children's negligence/negligence *per se*, breach of implied contract and unjust enrichment.

9. Additionally, given the scope of sensitive data compromised by Lurie Children's, offering a mere 24 months of credit monitoring is insufficient to protect and remediate the harm caused by Lurie Children's violations of law - Plaintiff and the putative Class seek at least three years of identity theft protection and credit monitoring.

II. JURISDICTION AND VENUE

10. **Subject Matter Jurisdiction.** This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount of controversy easily exceeds the sum of \$5,000,000 exclusive of interests and costs, there are more than 100 putative Class members, and minimal diversity exists because many of the putative Class members are citizens of a different state than Defendant.

11. **Personal Jurisdiction.** This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in Chicago, Illinois. Furthermore, Defendant intentionally availed itself of this jurisdiction by marketing, employing individuals, and providing services in Illinois.

12. **Venue.** Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant operates in this District and a substantial part of the events, acts and omissions giving rise to Plaintiff's claims occurred here, in this District.

III. PARTIES

Plaintiff C.K.

13. Plaintiff C.K., a minor, is a resident and citizen of the State of Illinois and intends to remain domiciled in and a citizen of the State of Illinois.

Defendant Ann & Robert H. Lurie Children's Hospital of Chicago

14. Defendant Lurie Children's is a Chicago-based, Illinois entity located in 54 locations spread out throughout Illinois and the general area, with its principal place of business located at 225 E. Chicago Avenue, Chicago, Illinois 60611.

IV. FACTUAL ALLEGATIONS

Defendant's Business

15. Lurie Children's is a major hospital system domiciled in Illinois, serving patients in Illinois, Wisconsin, Indiana, and the surrounding area. Lurie Children's has over 50 locations spread throughout the region and provides a multitude of healthcare-type services for pediatric patients.

16. In the ordinary course of receiving health care services from Lurie Children's, patients are required to provide, at a minimum, the PII, which is the data set of information compromised in this Data Breach, as previously stated.

17. Prior to receiving care and treatment from Lurie Children's, Plaintiff was required to and did in fact turn over much (if not all) of the private and confidential information listed above.

18. Additionally, with respect to medical care and protected health information, Lurie Children's may receive private and personal information from other individuals and/or

organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

19. Lurie Children's also likely creates and maintains a considerable amount of PHI in the course of providing medical care and treatment. This PHI includes, but is not limited to, billing account numbers, financial information, medical record numbers, dates of service, provider names, and medical and clinical treatment information regarding care received from Lurie Children's.

20. According to Lurie Children's Privacy Policy, Lurie Children's provides each of its patients with a HIPAA compliant notice of its privacy practices in respect to how they handle patients' sensitive and confidential information.

21. A copy of the Privacy Policy is maintained on Lurie Children's website.

22. Lurie Children's promises to maintain the confidentiality of patients' health, financial, and non-public personal information, ensure compliance with federal and state laws and regulations, and not to use or disclose patients' health information for any reasons other than those expressly listed in the Privacy Policy without written authorization.

23. As a condition of receiving services and/or employment from Defendant, Defendant requires that its patients entrust it with highly sensitive personal information.

24. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

25. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

26. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for employment, business and health purposes only, and to make only authorized disclosures of this information.

The Data Breach

27. On or about June 28, 2024, Lurie Children's notified victims of the Data Breach. This was done in part by disseminating the Notice as well as a notification on Defendant's website. The notification on Defendant's website reads as follows:

Ann & Robert H. Lurie Children's Hospital of Chicago ("Lurie Children's") has been investigating the nature and scope of a sophisticated cybersecurity attack that occurred earlier this year. Throughout our response to this matter, Lurie Children's has remained dedicated to the care and safety of our patients.

Through Lurie Children's' ongoing investigation, we have determined that cybercriminals accessed Lurie Children's systems between January 26 and 31, 2024. On January 31, 2024, to protect our systems and our ability to continue operations, Lurie Children's took certain electronic systems offline, including our email, phones, and electronic health record system (Epic), and its patient portal (MyChart). Lurie Children's also activated our standard incident response procedures, including the Hospital Incident Command Structure (HICS). The Hospital implemented its downtime procedures, and we have remained open for patient care throughout the investigation. Additionally, we retained leading cybersecurity experts and legal counsel to work with our internal teams. We have worked closely with law enforcement as well.

Due to the complexity of the attack as well as our infrastructure, it has taken time to understand what happened and to identify the scope of impact to our systems and data. As part of our ongoing investigation, we thoroughly and methodically reviewed and analyzed impacted data contained on those systems. Through our investigation, Lurie Children's has determined that information relating to certain individuals, such as name, address, date of birth, dates of service, driver's license number, email address, health claims information, health plan, health plan beneficiary number, medical condition or diagnosis, medical record number, medical treatment, prescription information, Social Security number, and telephone number, was impacted. The information relating to a particular individual varies individual to individual. We have no indication that the cybercriminals accessed data stored in our electronic health record system (Epic), although certain information stored in other Lurie Children's systems was impacted.

At Lurie Children's, we take seriously the privacy of our patients' and team members' sensitive information. Lurie Children's did not pay a ransom. Experts have advised that making a payment to cybercriminals does not guarantee the deletion or retrieval of data that has been taken. Once our investigation team identified an amount of data that was impacted by the cybercriminals, we worked closely with law enforcement to retrieve that data.

Lurie Children's is in the process of notifying individuals whose data was impacted, including through mailing notification letters and other methods. Our notification material will identify resources to help protect their identity. Additionally, Lurie Children's is offering individuals whose data was impacted complimentary access to Experian IdentityWorksSM for 24 months to help protect their information. Lurie Children's serves patients and patient families around the world, and individuals who live outside of the United States may receive those services if they're available in their country.

It is always a good practice to remain vigilant and to carefully review your online accounts, financial statements, and Explanations of Benefits from your health insurers for any unauthorized activity. Contact the company that maintains the account immediately if you detect any suspicious transactions or other activity you do not recognize.

Lurie Children's has established an external toll-free call center to address the community's questions about notification, the cybersecurity attack and our response. If you have additional questions about the notification, any notification letter you may have received, or whether your information was impacted, you can contact the call center at [888-401-0575](tel:888-401-0575), Monday-Friday between 8 am and 8 pm, U.S. central time.

We deeply regret that this cybersecurity attack occurred. Hospitals and health systems across the country face constantly evolving cybersecurity threats. For our part, we are working closely with our internal and external experts to further enhance the security of our systems.

We remain incredibly grateful for the support and patience of our patients, patient-families, team members, community partners, research partners and broader Lurie Children's community throughout this matter. We look forward to continuing our longstanding mission of creating a healthier future for every child.

28. The notice related to this Data Breach raises significantly more questions than it answers.

29. Critically, Lurie Children's waited over five months until June 27, 2024 to inform its patients that their PII and PHI could be compromised as a result of the Data Breach. This critical passage of time is and was harmful to the victims of the Data Breach. As is the case with data breaches generally, every moment is precious in order to recover data and take necessary safety measures to insulate from the many harms that data breaches cause.

30. Lurie Children's omissions within the Notice are also important: Lurie Children's fails to illuminate how the unauthorized actors initially gained access, why Lurie Children's failed to detect the intrusion(s) of these unauthorized actors, and specifically how Lurie Children's intends to avoid making these types of incidents from happening again. These critical points remain unclear.

31. But what's clear from the Notice is that cybercriminals did, in fact, perpetrate a ransomware attack, then proceeded to access and view Plaintiff's and Class members' PII and PHI during the time period in which the cybercriminals had unfettered access to Defendant's IT network, as that is the *modus operandi* of cybercriminals who commit such attacks.

32. Simply, Defendant could have prevented this Data Breach.

33. Defendant did not implement or maintain adequate measures to protect its current and former patients' PII and PHI.

34. On information and belief, the PII and PHI compromised in the files accessed by hackers was not encrypted – this can be presumed given the hackers were able to access the data that was stated as compromised in the Notice.

35. Moreover, the removal of PHI and other PII and PHI from Defendant's system demonstrates that this cyberattack was targeted due to Defendant's status as a healthcare facility that houses sensitive PII and PHI.

36. Due to Defendant's incompetent security measures and their incompetent response to the Data Breach, Plaintiff and the Class Members now face a present and substantial risk of fraud and identity theft and must deal with that threat forever.

37. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII and PHI, the sophistication of Defendant, and the fact that Defendant is well aware of the risks of healthcare data breaches (as Defendant has an entire page on their website analyzing healthcare data breaches on a monthly basis), Defendant provided unreasonably deficient protections prior to the Breach, including, but not limited to a lack of security measures for storing and handling patients' PII and PHI and inadequate employee training regarding how to access, handle and safeguard this information.

38. This could have only occurred because Defendant failed to adequately adopt and train its employees on even the most basic of information security protocols, including: storing, locking encrypting and limiting access to current and former patients' highly sensitive PHI; implementing guidelines for accessing, maintaining and communicating sensitive PHI, and protecting sensitive PHI by implementing protocols on how to utilize such information.

39. Defendant's failures caused the unpermitted disclosure of Plaintiff's and Class members' PII to an unauthorized third party and put Plaintiff and the Class at serious, immediate and continuous risk of identity theft and fraud.

40. The Data Breach that exposed Plaintiff's and Class members' PHI was caused by Defendant's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes.

41. Defendant failed to comply with security standards or to implement security measures that could have prevented or mitigated the Breach.

42. Defendant failed to ensure that all personnel with access to its patients' PII and PHI were properly trained in retrieving, handling, using and distributing sensitive information.

The Breach Was Entirely Foreseeable

43. Defendant had obligations created by HIPAA, industry standards, common law and its own promises and representations made to Plaintiff and Class Members to keep their PII and PHI confidential and to protect it from unauthorized access and disclosure.

44. Plaintiff and Class members provided their PII and PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

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

46. Data breaches, including those perpetrated against the healthcare sector of the economy, have become extremely widespread.

47. Lurie Childrens' data security obligations were particularly important given the substantial increase in ransomware attacks and/or data breaches in the healthcare industry preceding the date of the Data Breach.

48. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread. Not surprisingly, healthcare is by far the most affected industry sector by data breaches and ransomware incidents. According to HIPAA statistics, between 2009 and 2022, 5,150 healthcare data breaches of 500 victims or more occurred. And, of those breaches, the impermissible disclosure of 382,262,109 healthcare records occurred. The rate of healthcare-related data breaches have also accelerated, with an average of approximately one

large (500 victims or more) healthcare-related data breach per day in 2018 as compared to nearly two such data breaches per day in 2022. In 2023 alone, there were many large healthcare-related data breaches with tens of millions of victims including the MOVEit data breaches (tens of millions of victims across multiple data breaches), HCA Healthcare (11,270,000 victims), Perry Johnson & Associates (11,000,000+ victims), MCNA Dental (8,861,076 victims), and others. As such, Lurie Children's was aware of the risk of data breaches because such breaches have dominated the headlines recently.

49. There is substantial evidence that data breaches in the healthcare sector harm patient outcomes. According to a 2019 Cornell University study titled "Do Hospital Data Breaches Reduce Patient Care Quality," "[h]ospital data breaches significant increase ... mortality rate[.] Data breaches may disrupt the processes of care that rely on health information technology. Financial costs to repair a breach may also divert resources away from patient care. Thus, breached hospitals should carefully focus investments in security procedures, processes, and health information technology that jointly lead to better data security and improved patient outcomes."

50. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals... because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

51. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.

52. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”

53. According to the 2019 Health Information Management Systems Society, Inc. (“HIMMS”) Cybersecurity Survey, “[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets.”

54. PII and PHI is of great value to hackers and cybercriminals, and the data compromised in the Breach can be used in a variety of unlawful manners.

55. PII and PHI can be used to distinguish, identify or trace an individual’s identity, such as their name and medical records.

56. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace and mother’s maiden name.

57. Given the nature of this Data Breach, it is foreseeable that the compromised PII and PHI can be used by hackers and cybercriminals in a variety of different ways.

58. Indeed, the cybercriminals who possess the Class members’ PII and PHI can readily obtain Class members’ tax returns or open fraudulent credit card accounts in the Class members’ names.

59. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including, upon information and good faith belief, to the Defendant.

Defendant Failed to Follow FTC Guidelines

60. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

61. According to the FTC, the need for data security should be factored into all business decision-making.

62. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

63. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.

64. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

65. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

68. Defendant failed to properly implement basic data security practices.

69. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to patients’ PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

70. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Meet Industry Standards

71. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

72. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software;

encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

73. Other best cybersecurity 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.

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

75. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant Failed to Comply with HIPAA

76. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

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

78. Title II of HIPAA contains what are known as the Administrative Simplification provisions. These provisions require, among other things, that the Department of Health and Human Services (“HHS”) create rules to streamline the standards for handling PHI and PII like the data Defendant left unguarded.

79. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D) and 45 C.F.R. § 164.530(b).

A data breach such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule: A breach under the HIPAA Rules is defined as, “...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” See 45 C.F.R. 164.40

80. Data breaches are Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

The presence of ransomware (or any malware) on a covered entity’s or business associate’s computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).

81. Defendant’s Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

Defendant's Breach

82. Defendant breached its obligations to Plaintiff and the Class members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, network and data.

83. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect consumers' PHI and other PII and PHI;
- c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts and clearing of event logs;
- d. Failing to apply all available and necessary security updates;
- e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;
- f. Failing to practice the principle of least-privilege and maintain credential hygiene;
Failing to avoid the use of domain-wide, admin-level service accounts;
- g. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;
- h. Failing to properly train and supervise employees in the proper handling of inbound emails;
- i. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

- j. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- k. 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)(i);
- l. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- m. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- n. Failing to protect against 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);
- o. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);
- p. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b) and/or;
- q. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI 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,” 45 CFR § 164.304 (definition of encryption).

84. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff’s and the Class members’ PII and PHI.

85. Accordingly, as outlined below, Plaintiff and Class members now face a substantial, increased, and immediate risk of fraud and identity theft.

Data Breaches Are Disruptive and Harm Consumers

86. Hacking incidents and data breaches at medical facilities and companies like Defendant are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

87. As previously stated, researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.

88. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.

89. The United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”

90. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

91. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

92. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number.

93. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

94. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.¹¹

95. Theft of PII and PHI is gravely serious. PII and PHI is an extremely valuable property right.

96. Its value is axiomatic, considering the value of “big data” in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII and PHI has considerable market value.

97. Theft of PHI, in particular, is gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”

98. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds’ medical insurance premiums.

99. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when PII, PHI, and/or financial information is stolen and when it is used.

100. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. See GAO Report, at p. 29.

101. PII and PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

102. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

103. Thus, Plaintiff and Class members must vigilantly monitor their financial and medical accounts for many years to come.

104. Sensitive PII and PHI can sell for as much as \$363 per record according to the Infosec Institute.

105. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

106. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

107. Medical information is especially valuable to identity thieves.

108. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.

109. Because of the value of its collected and stored data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

110. For this reason, Defendant knew or should have known about these dangers and strengthened its network and data security systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Harm to Plaintiff

111. On or about June 27, 2024, Plaintiff C.K.'s guardian became cognizant of the Data Breach as alleged herein.

112. As a result of the Data Breach, Plaintiff's guardian made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff's guardian has spent several hours dealing with the Data Breach by reviewing medical statements produced by payors/insurers, valuable time Plaintiff otherwise would have spent on other activities.

113. Plaintiff suffered actual injury from having her son's PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

114. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

115. This Action is properly maintainable as a Class Action.

116. Plaintiff brings this Action on behalf of himself and all similarly situated persons for the following Class defined as:

Class Definition. All individuals and entities residing in the United States whose PII and/or PHI was compromised on the Data Breach first announced by the Defendant on June 27, 2024.

(collectively, the “Class”).

117. Excluded from the Classes are: Defendant and Defendant’s relatives, subsidiaries, affiliates, officers and directors, and any entity in which the Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

118. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

119. Numerosity. Defendant reports that the Data Breach compromised PHI of nearly 800,000 current and former patients. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

120. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost or disclosed Plaintiff’s and Class Members’ PII;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant’s data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant’s data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

k. Whether Defendant failed to provide notice of the Data Breach in a timely manner and

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, equitable relief and/or injunctive relief.

121. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's PHI, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by Defendant's uniform conduct. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

122. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class in that he has no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel

experienced in complex consumer class action litigation, including, but not limited to, similar data breach class action litigation, and Plaintiff intends to prosecute this action vigorously.

123. Superiority of Class Action. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

124. The litigation of the claims brought herein is manageable. Lurie Children's uniform conduct, the consistent provisions of the relevant laws and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

125. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

126. Predominance. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

127. This proposed class action does not present any unique management difficulties.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

NEGLIGENCE

128. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

129. Defendant required Plaintiff and the Class Members to submit non-public personal information in order to obtain medical services.

130. The Class members are individuals who provided certain PII and PHI to Defendant including, and at a minimum, the PII and PHI described above.

131. Defendant had full knowledge of the sensitivity of the PII and PHI to which it was entrusted and the types of harm that Class members could and would suffer if the information were wrongfully disclosed.

132. Defendant had a duty to each Class member to exercise reasonable care in holding, safeguarding and protecting that information.

133. Plaintiff and the Class members were the foreseeable victims of any inadequate safety and security practices.

134. The Class members had no ability to protect their data in Defendant's possession.

135. By collecting and storing this data in its computer property, and by sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and the Class members' PII and PHI held within it — to prevent disclosure of the information and to safeguard the information from theft.

136. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

137. Defendant owed a duty of care to safeguard the PII and PHI of Plaintiff and Class members in its custody. This duty of care arises because Defendant knew of a foreseeable risk to the data security systems it used. Defendant knew of this foreseeable risk because of the explosion of data breach incidents involving healthcare providers detailed above. Despite its knowledge of this foreseeable risk, Defendant failed to implement reasonable security measures.

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

139. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as the common law.

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

141. Defendant's conduct also rises to the level of Negligence *per se*.

142. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

143. Some or all of the medical information at issue in this case constitutes “protected health information” within the meaning of HIPAA.

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

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

146. Defendant breached its duties, and thus was negligent (as well as negligent *per se*), by failing to use reasonable measures to protect the Class members’ PHI and PII.

147. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

- a. Failing to adopt, implement and maintain adequate security measures to safeguard Class members’ PII and PHI;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class members’ PII and PHI;
- e. Failing to detect in a timely manner that Class members’ PII and PHI had been compromised;
- f. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages and
- g. Failing to have mitigation and back-up plans in place in the event of a cyber- attack and data breach.

148. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' PII and PHI would result in injury to Plaintiff and Class members.

149. Further, the breach of security was reasonably foreseeable given the known high frequency of hacking incidents, cyberattacks, and data breaches in the healthcare industry.

150. It was therefore foreseeable that the failure to adequately safeguard Class members' PII and PHI would result in one or more types of injuries to Class members.

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

152. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures and (iii) provide adequate credit monitoring to all Class members.

SECOND CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

153. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

154. Defendant provides medical treatment and care to Plaintiff and Class members. Defendant formed an implied contract with Plaintiff and Class members through their collective conduct.

155. Through Defendant's provision of services, it knew or should have known that it must protect Plaintiff's and Class members' confidential PII and PHI in accordance with Defendant's stated policies, practices and applicable law.

156. As consideration, Plaintiff and Class members turned over valuable PII and PHI in

exchange for either medical services or care.

157. Defendant accepted possession of Plaintiff's and Class members' PII and PHI for the purpose of providing services to Plaintiff and the Class members. In delivering their PII and PHI to Defendant, Plaintiff and the Class members intended and understood that Defendant would adequately safeguard the PII as part of the provision or receipt of those services.

158. Defendant's implied promises to Plaintiff and Class members include, but are not limited to Defendant: (1) taking steps to ensure that anyone who is granted access to PII and PHI also protects the confidentiality of that data; (2) taking steps to ensure that the PII and PHI placed in control of Defendant's employees is restricted and limited only to achieve authorized business purposes; (3) restricting access to employees and/or agents who are qualified and trained; (4) designing and implementing appropriate retention policies to protect PII and PHI; (5) applying or requiring proper encryption and/or the separation of different data sets; (6) implementing multifactor authentication for access; and (7) taking other steps to protected against foreseeable breaches.

159. Plaintiff and Class members would not have entrusted their PII and PHI to Defendant in the absence of such an implied contract.

160. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class members' PII and PHI.

161. Plaintiff and Class members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein. Plaintiff seeks damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION

UNJUST ENRICHMENT

162. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

163. This Count is alternatively pled to Count III, Breach of Implied Contract.

164. Plaintiff and Class Members conferred a benefit on Defendant with their money or labor services. Specifically, they purchased goods and services from Defendant and/or provided their labor and in so doing also provided Defendant with their PII and PHI. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and should have had their PII and PHI protected with adequate data security.

165. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiff and Class Members for business purposes.

166. In particular, the Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. 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.

167. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed

to implement appropriate data management and security measures that are mandated by industry standards.

168. Defendant failed to secure Plaintiff's and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

169. Defendant acquired the PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

170. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

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

172. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their PII and PHI is used; (c) the compromise, publication, and/or theft of their PII and PHI; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII and PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

173. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

174. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

VII. PRAYER FOR RELIEF

175. WHEREFORE, Plaintiff, on his own and behalf of all others similarly situated, pray for relief as follows:

- A. For an Order certifying this case as a class action and appointing Plaintiff and his counsel to represent the Class;
- B. For an award of actual damages, compensatory damages, statutory damages, nominal damages and statutory penalties, in an amount to be determined, as allowable by law;
- C. For an award of damages, equitable, and injunctive relief, as well as reasonable attorneys' fees and costs, on behalf of themselves and the Class.
- D. For an award of punitive damages, as allowable by law;
- E. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the class which remains in Defendant's possession.
- F. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- G. Pre- and post-judgment interest on any amounts awarded; and
- H. Such other and further relief as the Court may deem just and proper.

VIII. JURY TRIAL DEMAND

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

DATED: June 28, 2023

Respectfully Submitted,

/s/ Blake Hunter Yagman

Blake Hunter Yagman

Edward Ciolko*

Jennifer Czeisler*

STERLINGTON PLLC

One World Trade Center, 85th Floor

New York, New York 10007

Tel.: 212-739-0622

Fax: 212-739-0628

Email: blake.yagman@sterlingtonlaw.com

ed.ciolko@sterlingtonlaw.com

jen.czeisler@sterlingtonlaw.com

Michael C. Lueder (NDIL Trial Bar)

HANSEN REYNOLDS LLC

301 N. Broadway, Suite 400

Milwaukee, Wisconsin 53202

Tel.: 414-273-8474

Email: mlueder@hansenreynolds.com

*Pro Hac Vice Forthcoming

Attorneys for Plaintiff C.K. and the Proposed Class

The ILND 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

(b) County of Residence of First Listed Plaintiff (Except in U.S. plaintiff cases)

(c) Attorneys (firm name, address, and telephone number)

DEFENDANTS

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 (Check one box, only.)

- 1 U.S. Government Plaintiff, 2 U.S. Government Defendant, 3 Federal Question, 4 Diversity

III. CITIZENSHIP OF PRINCIPAL PARTIES (For Diversity Cases Only.)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship and incorporation status.

IV. NATURE OF SUIT (Check one box, only.)

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, SOCIAL SECURITY, FEDERAL TAXES, OTHER STATUTES.

V. ORIGIN (Check 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, 6 Multidistrict Litigation - Transfer, 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION (Enter U.S. Civil Statute under which you are filing and write a brief statement of cause.)

VII. PREVIOUS BANKRUPTCY MATTERS (For nature of suit 422 and 423, enter the case number and judge for any associated bankruptcy matter previously adjudicated by a judge of this Court. Use a separate attachment if necessary.)

VIII. REQUESTED IN COMPLAINT:

Check if this is a class action under Rule 23, F.R.C.V.P.

Demand \$

CHECK Yes only if demanded in complaint:

Jury Demand: Yes No

IX. RELATED CASE(S) IF ANY (See instructions):

Judge

Case Number

X. Is this a previously dismissed or remanded case?

Yes No If yes, Case #

Name of Judge

Date:

Signature of Attorney of Record

Authority for Civil Cover Sheet

The ILND 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
(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
(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" 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 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.
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.