E-FILED
Monday, 25 November, 2024 01:38:53 PM
Clerk, U.S. District Court, ILCD

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS

IN RE: HOSPITAL SISTERS HEALTH SYSTEM DATA SECURITY LITIGATION	**CLASS ACTION COMPLAINT**
Defendant.	Case No.: 3:24-cv-03253
	JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Sandra McCoy, Kim Wade, Nick Avery, and Charles Bovard (collectively, "Plaintiffs"), individually and on behalf of the Class of similarly situated persons, assert claims against Defendant Hospital Sisters Health System ("Defendant" or "HSHS") and allege the following based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by counsel as to all other matters:

SUMMARY OF THE CASE

1. This action arises from Defendant's failure to secure the personally identifiable information ("PII")[1] and protected health information ("PHI")[2] (collectively, "Private

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS.,

Information") of Plaintiffs and the members of the proposed Class.

2. HSHS is a health care system comprised of 13 hospitals, 1,000 plus physician partners, and more than 11,000 colleagues. Defendant operates in Illinois, Wisconsin, and several other locations across the country.[3]

3. Between August 16, 2023, and August 27, 2023, HSHS experienced a cybersecurity incident. After conducting an investigation, HSHS determined that an unauthorized third-party accessed certain files off its system, which contained the Private Information of Plaintiffs and Class Members (the "Data Breach").

4. The Private Information intruders accessed and infiltrated from Defendant's systems included, names, addresses, dates of birth, Social Security numbers, driver's license numbers, medical record numbers, and/or limited medical, health insurance and/or limited treatment information related to care received at HSHS.

5. As a result of the Data Breach, which Defendant failed to prevent, the Private Information of its patients, including Plaintiffs and the proposed Class Members, was stolen.

6. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard its current and former patients' Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. Defendant's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

7. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly

---

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Nov. 22, 2024).

[3] https://www.hshs.org/about-us (last visited Nov. 22, 2024).

impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) expense and time spent on initiating fraud alerts and contacting third parties; (k) decreased credit scores; (l) lost work time; (m) anxiety, annoyance, and nuisance; and (n) continued risk to their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

8. Plaintiffs and Class Members would not have provided their valuable Private Information had they known that Defendant would make their Private Information Internet-accessible, not encrypt personal and sensitive data elements and not delete the Private Information it no longer had reason to maintain.

9. Through this lawsuit, Plaintiffs seek to hold Defendant responsible for the injuries they inflicted on Plaintiffs and Class Members due to its impermissibly inadequate data security measures, and to seek injunctive relief to ensure the implementation of security measures to protect the Private Information that remains in Defendant's possession.

10. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiffs' and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

JURISDICTION AND VENUE

11. The 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 about 180,000 people, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

12. The Court has general personal jurisdiction over Defendant because Defendant's headquarters and principal place of business is located at 4936 Laverna Road Springfield, IL 62707.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391, because it is the District within which Defendant has the most significant contacts.

PARTIES

14. Plaintiff Sandra McCoy is, and at all relevant times has been, a resident and citizen of the State of Illinois, where she intends to remain.

15. Plaintiff Kim Wade is, and at all relevant times has been, a resident and citizen of the State of Illinois, where she intends to remain.

16. Plaintiff Nick Avery is, and at all relevant times has been, a resident and citizen of the State of Illinois, where he intends to remain.

17. Plaintiff Charles Bovard is, and at all relevant times has been, a resident and citizen of the State of Illinois, where he intends to remain.

18. Defendant Hospital Sisters Health System is an Illinois corporation with its headquarters and principal place of business located at 4936 Laverna Road Springfield, IL 62707.

FACTUAL ALLEGATIONS

A. The Data Breach

19. As a condition of receiving treatment, Plaintiffs and Class Members were required to provide HSHS with their sensitive and confidential Private Information, including their names, Social Security numbers, and other sensitive information, that would be held by Defendant in its computer systems.

20. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

21. As evidenced by the Data Breach, the Private Information was contained in Defendant's network and was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

B. The Dark Web Is Used by Cybercriminals to Share and Sell Private Information

22. The dark web is a part of the World Wide Web that is not accessible through traditional internet browsers. The term "dark web" is used to distinguish from the "clear web," the part of the World Wide Web that is readily accessible through traditional internet browsers. The dark web is accessed through The Onion Router ("Tor"), a privacy-focused communication system designed to enable anonymous internet browsing. It achieves this by routing web traffic through multiple volunteer-operated servers (relays), encrypting data at each step to ensure that both the user's location and browsing activity are difficult to trace. Tor uses a technique called onion routing, where data is encrypted in layers like an onion. Each relay in the network peels away a

layer of encryption before passing the data to the next relay. This ensures that no single relay knows both the origin and destination of the data.

23. Tor is based on an earlier protocol developed by the U.S. Navy, specifically for military applications. The basic concepts for onion routing were developed at the U.S. Naval Research Laboratory in the mid-1990s and later refined by the Defense Advanced Research Projects Agency (DARPA) with the goal of providing secure intelligence communication online.[4]

24. When using Tor, a user's IP address is masked, and their internet traffic is routed through a series of relays before reaching the destination.[5] This makes it difficult for websites, internet service providers, or third parties to track the user's real IP address or browsing activity.[6] One can access the Tor network using a Tor browser, which is a free modified version of the Mozilla Firefox browser.[7]

25. This process of onion routing makes for a level of anonymity that is not readily available on traditional web sites.[8] While one can utilize a fake identity on a clear web site, the website may track the user's IP address, thus revealing who the user is. Onion routing makes the entire communication process anonymous.

---

[4] Kyle Swan, *Onion Routing and tor*, Georgetown Law Technology Review (2020), https://georgetownlawtechreview.org/onion-routing-and-tor/GLTR-11-2016/ (last visited Nov 22, 2024).

[5] Mastrostefano, *Onion under Microscope: An in-depth analysis of the Tor network*, NASA/ADS (Jan. 2021), https://ui.adsabs.harvard.edu/abs/2021arXiv210108194B/abstract.

[6] Dimitris Simos, *On Combinatorial Security Testing for the Tor Anonymity Network Client*, NIST (Apr. 7, 2024), https://www.nist.gov/publications/combinatorial-security-testing-tor-anonymity-network-client.

[7] *The Tor Project*, https://www.torproject.org/download.

[8] Ben Collier, *Tor: From the Dark Web to the Future of Privacy*, MIT Press (2024), https://direct.mit.edu/books/oa-monograph/5761/TorFrom-the-Dark-Web-to-the-Future-of-Privacy.

26. Websites accessible only via Tor have addresses that end in ".onion." For example, the address http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/ is a popular dark web search engine. These sites can only be accessed via the Tor browser.

27. The dark web poses significant challenges to cyber security professionals and law enforcement agencies. The dark web is legal to access and operate, and it has some legitimate applications and sites. But its hidden nature and employment of multi-level encryption make detecting and monitoring illegal activity difficult. Unlike the clear web, dark web sites do not advertise their existence.

28. Some dark web sites are simply places for people who wish to avoid tracking while browsing the World Wide Web.[9] However, the anonymity of the dark web has led to the creation of a number of markets and forums which traffic in illegal merchandise and content, including stolen Private Information.[10]

29. Once stolen Private Information is posted on the dark web, it will most likely be distributed to multiple different groups and individuals, each of which can use that information for fraud and identity theft.[11]

30. This data lifecycle has also been confirmed with experiments. In 2015, researchers at BitGlass created a list of 1,568 phony names, Social Security numbers, credit card numbers, addresses, and phone numbers, rolled them in an Excel spreadsheet, and then "watermarked" it

---

[9] Thomas J. Holt, *Open, Deep, and Dark: Differentiating the Parts of the Internet Used For Cybercrime*, Michigan State University, School of Criminal Justice, https://cj.msu.edu/_assets/pdfs/cina/CINA-White_Papers-Holt_Open_Deep_Dark.PDF.

[10] *Crime and the Deep Web*, Stevenson University, https://www.stevenson.edu/online/about-us/news/crime-deep-web/; *Defending Against Malicious Cyber Activity Originating from Tor*, CISA (Aug. 2, 2021), https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a.

[11] *The Dark Web and Cybercrime*, HHS Cybersecurity Program (July 23, 2020), https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf.

with their code that silently tracks any access to the file.[12] The data was quickly spread across five continents: North America, Asia, Europe, Africa, and South America. In the end, it was downloaded by 47 different parties. It was mainly downloaded by users in Nigeria, Russia, and Brazil, with the most activity coming from Nigeria and Russia.[13] This experiment demonstrated that data released on the dark web will quickly spread around the world.

C. Cybercriminals' data destruction promises cannot be trusted

31. The United States government and other law enforcement agencies almost always advise against paying a ransom demand sought by a cybercriminal, and that is because cybercriminals cannot be trusted to do what they promise they will do in exchange for a ransom.

32. These tactics are explicitly exploitative: they hinge on extracting monetary concessions from targets based on the dual desires to regain access to their stolen information and contain the impact of the data breach (and potential liability incurred therefrom).

33. Even in cases where organizations pay a ransom in exchange for decryption and/or promises not to post the stolen data on the clear web, there is no guarantee that the cybercriminals would honor their promises: the hackers could easily have re-copied the stolen data.[14]

---

[12] Kelly Jackson Higgins, *What Happens When Personal Information Hits The Dark Web*, (Apr. 7, 2015), https://www.darkreading.com/cyberattacks-data-breaches/what-happens-when-personal-information-hits-the-dark-web; *Dark Web*, Congressional Research Service (Mar. 10, 2017), https://crsreports.congress.gov/product/pdf/R/R44101;

[13] Pierluigi Paganini, *How far do stolen data get in the deep web after a breach?*, (Apr. 12, 2015), https://securityaffairs.com/35902/cyber-crime/propagation-data-deep-web.html.

[14] Gary Guthrie, *Paying to delete stolen data doesn't always work out for the victim, new study suggests*, ConsumerAffairs (Nov. 5, 2020), https://www.consumeraffairs.com/news/paying-to-delete-stolen-data-doesnt-always-work-out-for-the-victim-new-study-suggests-110520.html [https://perma.cc/DMV2-JRFP].

34. Indeed, data breach targets that pay ransom demands often cannot substantiate any claimed destruction or return of the data in question.[15]

35. The FBI recognizes the likelihood that cybercriminals will renege on their promises once a ransom is paid, explaining that it "does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data."[16]

36. Several media outlets and industry groups have likewise questioned reliance on promises made by cybercriminals.[17]

37. Indeed, HSHS's data breach notifications advised affected individuals to monitor their own credit and financial accounts for suspicious activity.

D. The Value of Private Information

38. Private Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" to corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of

---

[15] *See* Leo Kelion & Joe Tidy, *National Trust Joins Victims of Blackbaud Hack*, BBC News (July 30, 2020), https://www.bbc.com/news/technology-53567699 ("Although Blackbaud has said the cyber-criminals had provided confirmation that the stolen data was destroyed, one expert questioned whether such an assurance could be trusted. 'The hackers would know these people have a propensity to support good causes,' commented Pat Walshe from the consultancy Privacy Matters. This would be valuable information to fraudsters, he added, who could use it to fool victims into thinking they were making further donations when in fact they would be giving away their payment card details.") [https://perma.cc/NC7W-T9LJ]; *Phishing Scams Following Blackbaud Security Breach*, Mich. Dep't Att'y Gen., https://www.michigan.gov/ag/0,4534,7-359-81903_20942-540014--,00.html [https://perma.cc/E6K9-HVZZ].

[16] *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI (Oct. 2, 2019), https://www.ic3.gov/Media/Y2019/PSA191002 [https://perma.cc/VX8P-TW7F].

[17] *See, e.g.*, Phil Muncaster, *US Data Breach Volumes Plummet 30% in 2020*, Infosecurity Mag. (Oct. 15, 2020), https://www.infosecurity-magazine.com/news/us-data-breach-volumes-plummet-30/ [https://perma.cc/2LYC-XDP6]; Zack Whittaker, *Decrypted: The Major Ransomware Attack You Probably Didn't Hear About*, TechCrunch (Oct. 7, 2020), https://techcrunch.com/2020/10/07/decrypted-blackbaud-ransomware-attack-gets-worse/ [https://perma.cc/R8M4-FMMC].

$182.5 billion and net income of $40.2 billion.[18] $160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the Private Information it collects about users of its various free products and services.

39. Criminal law also recognizes the value of Private Information and the serious nature of the theft of PII by imposing prison sentences. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of Private Information. Once a cybercriminal has unlawfully acquired Private Information, the criminal can demand a ransom or blackmail payment for its destruction, use the Private Information to commit fraud or identity theft, or sell the PII to other cybercriminals on the black market.

40. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[19]

41. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary

[18] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

[19] https://www.zdnet.com/article/ransomeware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Nov. 22, 2024).

forms of extortion."[20]

42. Cybercriminals use "ransomware" to make money and harm victims. Ransomware is a widely-known and foreseeable malware threat in which a cybercriminal encrypts a victim's computer such that the computer's owner can no longer access any files or use the computer in any way. The cybercriminal then demands payment for the decryption key. Ransomware is typically propagated through phishing, spear phishing, or visiting a malicious or compromised website that contains a virus or other malware.

43. Stolen Private Information is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

44. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[21]

45. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [Private Information] belonging to victims from countries all over the world. One of the key challenges of protecting Private Information online is its pervasiveness. As data breaches in the news continue to show, Private Information about employees, customers and the public is housed in all kinds of organizations, and the

[20] *See* https://www.cisa.gov/news-events/news/cisa-and-ms-isac-release-joint-ransomware-guide (last visited Nov. 22, 2024).

[21] *Shining a Light on the Dark Web with Identity Monitoring, IdentityForce*, Dec. 28, 2020, https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Nov. 22, 2024).

increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[22]

46. The Private Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Private Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $2009.[23] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[24] Criminals can also purchase access to entire company data breaches.[25]

47. Once Private Information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional Private Information being harvested from the victim, as well as Private Information from family, friends and colleagues of the original victim.

---

[22] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited Nov. 22, 2024).

[23] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Nov. 22, 2024).

[24] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Nov. 22, 2024).

[25] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous- browsing/in-the- dark/ (last visited Nov. 22, 2024).

48. The U.S. Government Accountability Office ("GAO") released a report in 2007 regarding data breaches, finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

49. The GAO Report explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[27]

50. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[28] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a

---

[26] *Private Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[27] *Id.*

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

bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[29]

51. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[30]

52. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

53. Data breaches facilitate identity theft as hackers obtain consumers' Private Information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' Private Information to others who do the same.

54. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use Private Information to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[31] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and

---

[29] *See* Susan Henson, *What Can Identity Thieves Do with Your Private Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/askexperian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-youprotect-yourself/.

[30] https://www.ic3.gov/AnnualReport/Reports/2019_IC3Report.pdf (last visited Nov. 22, 2024)

[31] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf (last visited Nov. 22, 2024).

their] good name."[32]

55. The market for Private Information has continued unabated to the present, and in 2023 the number of reported data breaches in the United States increased by 78% over 2022, reaching 3205 data breaches.[33]

56. The exposure of Plaintiffs' and Class Members' Private Information to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit from this highly sensitive information.

57. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[34]

58. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

59. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to

---

[32] *Id*.

[33] Beth Maundrill, *Data Privacy Week: US Data Breaches Surge, 2023 Sees 78% Increase in Compromises*, INFOSECURITY MAGAZINE (Jan. 23, 2024); https://www.infosecurity-magazine.com/news/us-data-breaches-surge-2023/ (last visited Nov. 22, 2024); *see also* Identity Theft Resource Center, *2023 Data Breach Report*, https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited Nov. 22, 2024).

[34] *Id.*

find flaws in their computer systems, as stating: "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[35]

E. Defendant Failed to Comply with Regulatory Requirements and Standards.

60. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and employees. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

61. For example, at least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain Private Information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access.

62. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting of physical security systems; protecting against any possible communication system; and training staff regarding critical points.[36]

[35] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, Identity Theft Resource Center (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

[36] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://web.archive.org/web/20220629134548/https://insights.datamark.net/addressing-bpo-information-security

63. The FTC has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[37]

64. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[38]

65. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

66. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[39]

67. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or

---

[37] *Start With Security*, Fed. Trade Comm'n ("FTC"), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Nov. 22, 2024).

[38] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 22, 2024).

[39] *Id.*

practice barred by Section 5 of the Federal Trade Commission Act ("FTCA" or "FTC Act"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

68. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

69. Defendant's failure to verify that it had implemented reasonable security measures constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

70. Furthermore, Defendant is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

71. The Security Rule requires Defendant to do the following:

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

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

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

d. Ensure compliance by its workforce.[40]

72. Pursuant to HIPAA's mandate that HSHS follows "applicable standards,

[40] *Summary of the HIPAA Security Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Nov. 22, 2024).

implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302, HSHS was required to, at minimum, "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

73. HSHS is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

74. Both HIPAA and HITECH obligate HSHS to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

75. As alleged in this Complaint, HSHS has failed to comply with HIPAA and HITECH. It has failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of PHI.

F. Defendant Failed to Comply with Industry Practices.

76. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes

solutions to defend against those cyber-attacks.[41] All organizations collecting and handling Private Information, such as Defendant, are strongly encouraged to follow these controls.

77. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[42]

78. Several best practices have been identified that a minimum should be implemented by data management companies like Defendant, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[43]

79. Defendant failed to follow these and other industry standards to adequately protect the Private Information of Plaintiff and Class Members.

G. The Data Breach Could Have Been Prevented by Following Industry Standards for Data Security

80. HSHS could have prevented the Data Breach by following industry standards for secure software development and maintenance.

a. Secure software development

[41] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Nov. 22, 2024).

[42] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Nov. 22, 2024).

[43] *See* Center for Internet Security, *Critical Security Controls* (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Nov. 18, 2024).

81. HSHS could have prevented the Data Breach by following secure software development practices by default, rather than seeking to maintain and patch outdated software with critical security vulnerabilities.

82. Following secure software development practices from the beginning of development through release and maintenance of the software is an industry standard and best practice because it avoids the potential for overlooking a security vulnerability in outdated code.

83. HSHS failed to follow secure software development practices in developing and maintaining their networks because they included code with critical security vulnerabilities and then overlooked or did not attempt to discover such vulnerabilities when maintaining the software.

b. Monitoring potential security risks

84. HSHS could have prevented the Data Breach by monitoring potential security risks identified by the software development industry.

85. The software development industry publishes numerous resources for developers to learn about old, new, and emerging areas of potential vulnerability, such as the OWASP Top 10, which lists the 10 most serious potential security vulnerabilities in the industry today.

86. Monitoring developments in software security from industry resources is a best practice because it flags old, new, and emerging areas of potential vulnerability.

87. HSHS failed to monitor potential security risks because they maintained code with critical security vulnerabilities.

c. Sanitizing and validating user input

88. HSHS could have prevented the Data Breach by designing its code to sanitize and validate user input, rather than trusting user input as safe.

89. Sanitizing and validating user input is an industry standard and best practice because it ensures that data meets the criteria expected by the software, whether authorized or malicious, and stops potential sources of malicious code from reaching the database.

90. HSHS failed to sanitize and validate user input because they allowed unauthorized users to gain access to and compromise Personal Information stored on their networks.

d. Static code analysis

91. HSHS could have prevented the Data Breach by strictly analyzing their code for potential security vulnerabilities.

92. Static code analysis is an industry standard and best practice because it ensures that code is written in a manner that not only provides the expected output, but prevents unexpected or even harmful outputs.

93. Analysis of HSHS's code by a competent developer would have revealed glaring vulnerabilities that could have been removed before the Data Breach.

94. Third-party tools can analyze code for vulnerabilities that may be easy or hard to identify.[44]

95. HSHS failed to analyze its code for potential security vulnerabilities, instead blindly relying on poorly written code that performed as HSHS expected under controlled conditions.

e. Vulnerability testing

[44] Dave Wichers et al., *Source Code Analysis Tools*, OWASP, https://owasp.org/www-community/Source_Code_Analysis_Tools (last visited Nov. 22, 2024).

96. HSHS could have prevented the Data Breach by testing its code for potential security vulnerabilities, rather than simply using code that performed correctly under controlled conditions.

97. Vulnerability testing is an industry standard and best practice because it subjects code to scrutiny and unexpected user input so that critical flaws can be discovered.

98. Vulnerability testing involves subjecting software to extreme conditions that may be unexpected in the real world—such as sending improperly formatted requests to incorrect ports—to understand how the software reacts and whether any conditions can cause the software to fail or become insecure.[45]

99. Third-party tools can perform vulnerability testing by engaging in a range of interactions with the software while measuring performance.[46]

100. HSHS failed to analyze its code for potential security vulnerabilities, instead blindly relying on poorly written code that performed as HSHS expected under controlled conditions.

f. External penetration testing

101. HSHS could have prevented the Data Breach by subjecting their software to penetration testing by a third-party security firm.

102. Penetration testing is an industry standard and best practice because it subjects code to concerted attack scenarios that test its ability to withstand a data breach.

[45] Vitaly Unic, *Vulnerability Testing: Methods, Tools, and 10 Best Practices*, Bright (May 15, 2023), https://brightsec.com/blog/vulnerability-testing-methods-tools-and-10-best-practices/.

[46] *Id.*

103. Penetration testing is performed by third-party security firms with expertise in hacking software, whereby the firm attempts to compromise the software using a variety of tactics to test its resilience to an organized attack.

104. HSHS failed to perform penetration testing on its code, allowing the software to be used without any understanding of its ability to withstand an attempted data breach.

g. Organizations can take steps to mitigate the consequences of an imminent data breach

105. When faced with the urgent risk of a breach or data leak by cybercriminals, organizations can take specific steps to address both the immediate threat and longer-term security concerns.

106. Organizations that maintain sensitive data should have robust and tested incident response plans with clear protocols for handling ransomware and extortion attacks. A plan should include:

- Detection and isolation: Quickly identify and isolate compromised systems to contain the breach.[47]
- Monitor dark web threats actively: Organizations can monitor dark web forums for mentions of their data or breaches using threat intelligence tools. This allows for early detection of any data that might be posted and provides a heads-up if attackers begin selling stolen information.[48]

[47] *Incident Response Plan (IRP) Basics*, CISA, https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf; *How to Craft an Effective Incident Response Plan*, (Mar. 19, 2024), https://www.linkedin.com/pulse/how-craft-effective-incident-response-plan-thriveon-yyqmc.

[48] Esteban Borges, *Types of Cyber Crime: A Guide to Prevention & Impact*, Recorded Future (June 26, 2024), https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/types-of-cybercrime.

- Engage in proactive cyber hygiene: Regularly patch systems, enforce strong password policies, and limit access to sensitive data. This can make it harder for cybercriminals to penetrate systems or spread ransomware.[49]

- Prepare legal and public relations responses: Immediately involve legal counsel and public relations teams to prepare responses in case data is leaked. This includes engaging with regulators if needed and transparently informing affected stakeholders.[50]

- Conduct regular tabletop exercises: Practicing breach scenarios with response teams helps ensure readiness to act swiftly, especially if attackers set tight deadlines.[51]

H. The Data Breach Caused Injury to Class Members and Will Result in Additional Harm Such as Fraud

107. Without detailed disclosure to the victims of the Data Breach, individuals whose Private Information was compromised by the Data Breach, including Plaintiffs and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of their Private Information for months without being able to take available precautions to prevent imminent harm.

108. The ramifications of Defendant's failure to secure Plaintiffs' and Class Members' data are severe.

---

[49] *Vulnerability Management Best Practices*, (Sept. 28, 2023), https://www.wiz.io/academy/vulnerability-management-best-practices.

[50] Pádraig Walsh, *Data Breach Response: The Legal Team, External Counsel and Privilege*, Tanner DeWitt (July 6, 2021), https://www.tannerdewitt.com/data-breach-legal-team-external-counsel-privilege/; Daniel Solove, *The Biggest PR Mistake in Privacy and Data Security Incidents: An Interview with PR Expert Melanie Thomas*, (Aug. 11, 2014), https://www.linkedin.com/pulse/20140811174234-2259773-the-biggest-pr-mistake-in-privacy-and-data-security-incidents-an-interview-with-pr-expert-melanie-thomas; *Data Breach Response: A Guide for Business*, Federal Trade Commission (Apr. 29, 2019), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

[51] Ashley Watters, *The Importance of Realistic Tabletop Exercises*, (May 7, 2024), https://connect.comptia.org/blog/the-importance-of-realistic-tabletop-exercises.

109. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes.

110. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[52] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[53]

111. Identity thieves can use Private Information, such as that of Plaintiffs and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

112. As demonstrated herein, these and other instances of fraudulent misuse of the compromised Private Information have already occurred and are likely to continue.

113. As a result of Defendant's delay between the Data Breach in April and the notice of the Data Breach sent to affected persons in August, the risk of fraud for Plaintiff and Class Members increased exponentially.

114. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending

[52] 17 C.F.R. § 248.201 (2013).

[53] *Id*.

an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[54]

115. The 2017 Identity Theft Resource Center survey[55] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft; and
- 7% reported feeling suicidal.

116. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[56]

---

[54] *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 2015) https://bjs.ojp.gov/content/pub/pdf/vit14.pdf (last visited Nov. 22, 2024).

[55] https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Nov. 22, 2024)

[56] *Id*.

117. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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.[57]

Thus, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

I. Plaintiff and Class Members Suffered Damages.

118. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members have already been harmed by the fraudulent misuse of their Private Information, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

[57] GAO, *Report to Congressional Requesters*, at 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Nov. 22, 2024).

119. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and misused via the sale of Plaintiffs' and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. 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 Data Breach;

g. ascertainable losses in the form of deprivation of the value of their Private Information, for which there is a well-established national and international market;

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

i. nominal damages.

120. While Plaintiffs' and Class Members' Private Information has been stolen, Defendant continues to hold Plaintiffs' and Class Members' Private Information. Particularly because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and Class Members have an undeniable interest in ensuring that their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

121. Plaintiffs and Class Members have suffered injuries in a number of ways, including:

- Loss of benefit of their bargain;
- Loss of value of their personal information;
- Actual or attempted fraud, misuse, or identity theft; and
- Time and expenses that were reasonably spent to mitigate the impact of the breach.

122. Some Plaintiffs have already experienced actual or attempted fraud, which is reasonably related to the Data Breach, which demonstrates that the Data Breach has put them at immediate risk for additional harm.

123. The harm already suffered by Plaintiffs demonstrates that the risk of harm is ongoing.

J. It is reasonable for individual victims of cybercriminal data breaches to take actions to mitigate their risk of harm.

124. Cybercriminals can and do use the Private Information that HSHS was entrusted to safeguard to perpetrate financial crimes that harm Plaintiffs and the Class.

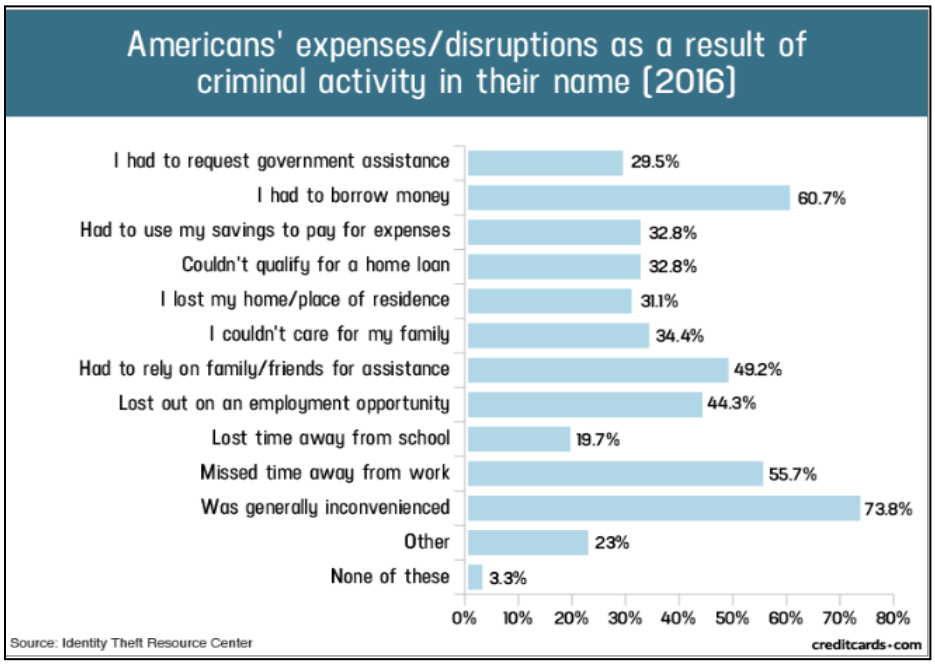
125. In addition to all the other immediate consequences of the Data Breach, Plaintiffs and Class Members face a substantially increased risk of identity theft and fraud.

126. The Federal Trade Commission ("FTC") recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), 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.[58]

[58] Identity Theft Recovery Steps, FTC, https://www.identitytheft.gov/Steps (last visited Mar. 23, 2021). Indeed, the FTC takes data breaches seriously, and has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information

127. Cybercriminals use stolen PII such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

128. A study by the Identity Theft Resource Center ("ITRC") shows the multitude of harms caused by fraudulent use of personal and financial information[59]:



129. As set forth above, 96.7% of study subjects experienced costs or other harms from the criminal activity.[60] As illustrated in the above graphic, this includes devastating results such as: "I lost my home/place of residence" and "I couldn't care for my family." Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC

---

can constitute an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[59] Jason Steele, Credit Card and ID Theft Statistics, Creditcards.com (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

[60] *Id.*

study, nearly one third of survey respondents had to request government assistance because of identity theft, such as welfare, EBT, food stamps, or similar support systems.[61] The ITRC study concludes that "identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual."[62]

130. PII is a valuable property right.[63] Its value is axiomatic, considering the value of Big Data in corporate America as well as the consequences of cyber thefts resulting in heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information has considerable market value that is diminished when it is compromised.

131. There may also be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the GAO Report: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[64]

132. PII is such an inherently valuable commodity to identity thieves that, once it is compromised, criminals often trade the information on the cyber black-market for years.

---

[61] *Id.*

[62] *Id.*

[63] *See, e.g.*, John T. Soma et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *1 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.").

[64] GAO Report at 29, *supra* note 245.

133. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[65]

134. Medical identity theft "is also more difficult to detect, taking almost twice as long as normal identity theft."[66] In warning consumers of the dangers of medical identity theft, the FTC states that an identity thief may use Private Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[67] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[68]

135. A report published by the World Privacy Forum[69] and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

---

[65] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[66] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[67] *See* FBI, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014) at 14, https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systemscyber-intrusions.pdf.

[68] *See* FTC, *What to Know About Medical Identity Theft*, FTC Consumer Information, https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited May 20, 2025).

[69] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017) at 24, https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

- Significant bills for medical goods and services not sought or received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgages or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

136. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (*e.g.*, donation history or hospital records), directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[70]

137. The United States Court of Appeals for the First Circuit has recognized that it is not necessary for a victim of a data breach to have their identity stolen, or to suffer actual fraud, for it to be reasonable for a data breach victim to take steps to protect themselves.[71]

---

[70] *See* Kelion & Tidy, *supra* note 241 (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

[71] *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 371 (1st Cir. 2023). In *Webb*, the First Circuit concluded that "plausible allegations of actual misuse [of PII] . . . state a concrete injury under Article III." *Webb*, 72 F.4th at 373. The First Circuit is in agreement with other circuits that

138. As the United States Court of Appeals for the Seventh Circuit aptly observed almost a decade ago: "the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[72]

139. This remains true, ten years later. The intent of hackers is clear when they hack systems, such as HSHS: they are attempting to access consumers' Private Information for the purpose of ransoming it back, and/or selling it for a profit.

140. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average, it takes approximately three months for a consumer to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[73]

141. In addition, there is a strong probability that much of the information stolen in the Data Breach has not yet been made available on the black market yet, meaning Plaintiffs and Class Members will remain at an increased risk of fraud and identity theft for many years into the future. Indeed, some Class Members are in very early stages of their lives—in their twenties and thirties. Thus, as the respective Data Breach Notices advise, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

K. Damages can compensate victims for the harm caused by the breach

---

have encountered the same question. *See, e.g.*, *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262 (11th Cir. 2021); *Attias v. CareFirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017); *In re Marriott, Int'l, Inc. Customer Data Sec. Breach Litig.,* 440 F. Supp. 3d 447, 459 (D. Md. 2020); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690 (7th Cir. 2015) ("customers should not have to wait until hackers commit identity theft or credit-card fraud" in order for their mitigation efforts to be reasonable and compensable).

[72] *Remijas*, 794 F.3d at 693.

[73] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

142. HSHS has refused to provide full compensation for harms caused by the Data Breach.

143. A year or two of credit monitoring will not un-ring the bell of the release of the Private Information of the Plaintiffs and Class Members, which will circulate through the various levels of the internet (clear, dark, and deep) for years and years, if not in perpetuity. Particularly considering the fact that Social Security numbers were exposed in the Data Breach, Data Breach victims will need to monitor their credit and accounts for years and years to come—and these services are typically accounted for in settlements and judgments involving data breaches.[74]

144. The Private Information exposed in the Data Breach has real value, as explained above. Plaintiffs and the Class have therefore been deprived of their rights to the control of that property and have lost the value they might otherwise have incurred from that data.[75]

145. Plaintiffs and the Class have spent significant time, and will spend more, monitoring their accounts, changing login credentials, and recovering from the inevitable fraud and identity theft which will occur, which deserves to be compensated.[76]

146. Similarly, HSHS has offered no compensation for the aggravation, agitation, anxiety, and emotional distress that Plaintiffs and the Class have suffered, and will continue to

---

[74] For instance, in July 2019, the CFPB, FTC and States announced a settlement with Equifax over the 2017 Equifax data breach, which included up to ten years of credit monitoring and identity restoration services. *See CFPB, FTC and States Announce Settlement with Equifax Over 2017 Data Breach*, CFPB (July 22, 2019), https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-states-announce-settlement-with-equifax-over-2017-data-breach/.

[75] Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS, May 14, 2021 https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it.

[76] Time spent monitoring accounts is another common and cognizable, compensated harm in data breach cases. *See* Equifax Data Breach Settlement FAQ, FTC, Dec. 2022, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

suffer, as a result of the Data Breach: the knowledge that their information is out in the open, available for sale and exploitation at any time in the future is a real harm that also deserves compensation.

147. Plaintiffs and members of the Class were also deprived of the benefit of their bargain when they interacted with HSHS, which had a duty to take reasonable steps to protect the Private Information of its patients. This duty was inherent in the relationships between Plaintiffs and Class Members and HSHS, whether through express contractual terms, implied contractual terms, or statutory or implied duties of good faith and fair dealing.

148. HSHS has not taken sufficient steps or even attempted to make their patients whole. HSHS has failed in its duty to protect Plaintiffs' and Class Members' Private Information and have failed in their duty to help these consumers protect themselves in the future.

L. Plaintiffs' Experiences.

Sandra McCoy

149. Plaintiff Sandra McCoy is a former patient of HSHS.

150. In order to become a patient of HSHS, she was required to provide Private Information to Defendant, including name, address, date of birth, Social Security number, driver's license number, medical record number, health insurance information, and medical and treatment information, and did so.

151. At the time of the Data Breach—between August 16 and August 27, 2023—Defendant retained Plaintiff McCoy's Private Information in its system.

152. Plaintiff McCoy is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet

or any other unsecured source.

153. Plaintiff McCoy would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

154. Plaintiff McCoy learned of the breach after receiving a letter from Defendant, on or about August 30, 2024, which told her that her Private Information had been accessed and compromised during the Data Breach. A copy of the Notice Letter is attached hereto as Exhibit 1.

155. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff McCoy made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and monitoring her accounts and credit reports for suspicious activity. Plaintiff McCoy has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

156. Plaintiff McCoy suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information..

157. The Data Breach has caused Plaintiff McCoy to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key

details about the Data Breach's occurrence.

158. As a result of the Data Breach, Plaintiff McCoy anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

159. 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.

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

Kim Wade

161. Plaintiff Wade is a former patient of HSHS.

162. In order to become a patient of HSHS, she was required to provide Private Information to Defendant, including her name, Social Security number, and address.

163. At the time of the Data Breach—between August 16 and August 27, 2023—Defendant retained Plaintiff Wade's Private Information in its system.

164. Plaintiff Wade is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

165. Plaintiff Wade would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

166. Plaintiff Wade learned of the breach after receiving a letter from Defendant, on or about August 30, 2024, which told her that her Private Information had been accessed and

compromised during the Data Breach. A copy of the Notice Letter is attached hereto as Exhibit 2.

167. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Wade made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter. Plaintiff Wade has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

168. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information..

169. The Data Breach has caused Plaintiff Wade to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

170. As a result of the Data Breach, Plaintiff Wade anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

171. 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.

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

Nick Avery

173. Plaintiff Nick Avery is a current patient of HSHS.

174. In order to become a patient of HSHS, he was required to provide Private Information to Defendant, including his name, Social Security number, and address.

175. At the time of the Data Breach—between August 16 and August 27, 2023—Defendant retained Plaintiff Avery's Private Information in its system.

176. Plaintiff Avery is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

177. Plaintiff Avery would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

178. Plaintiff Avery learned of the breach after receiving a letter from Defendant, on or about August 30, 2024, which told him that his Private Information had been accessed and compromised during the Data Breach. A copy of the notice letter is attached hereto as Exhibit 3.

179. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff Avery made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and self-monitoring accounts to ensure no fraudulent activity has occurred. Plaintiff Avery has spent significant time dealing with the Data

Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

180. Furthermore, Plaintiff has been a victim of fraud recently, in that an unknown third party attempted to open a credit card under his name, presumably providing his PII to do so. Plaintiff had to take many time-consuming steps to address and remedy the issue. Upon information and belief, this occurred because of the Data Breach.

181. As a result of the actual harm he has suffered and the present and increased imminent risk of future harm, Plaintiff spent time dealing with the fraud and reviewing his account statements. In addition, suffers from multiple health issues and is reasonably concerned his PHI has been exposed and is available to bad actors.

182. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

183. The Data Breach has caused Plaintiff Avery to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

184. As a result of the Data Breach, Plaintiff Avery anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

185. As a result of the Data Breach, Plaintiff Avery is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

186. Plaintiff Avery 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.

Charles Bovard

187. Plaintiff Charles Bovard is a former patient of HSHS.

188. In order to become a patient of HSHS, he was required to provide Private Information to Defendant, including his name, Social Security number, and address.

189. At the time of the Data Breach—between August 16 and August 27, 2023—Defendant retained Plaintiff Bovard's Private Information in its system.

190. Plaintiff Bovard is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

191. Plaintiff Bovard would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

192. Plaintiff Bovard learned of the breach after receiving a letter from Defendant, on or about August 30, 2024, which told him that his Private Information had been accessed and compromised during the Data Breach. A copy of the notice letter is attached hereto as Exhibit 4.

193. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff

Bovard made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and monitoring his accounts and credit reports for suspicious activity. Plaintiff Bovard has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

194. Plaintiff Bovard suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information..

195. The Data Breach has caused Plaintiff Bovard to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

196. As a result of the Data Breach, Plaintiff Bovard anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

197. As a result of the Data Breach, Plaintiff Bovard is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

198. Plaintiff Bovard has a continuing interest in ensuring that her Private Information,

which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

199. Plaintiffs bring this class action individually on behalf of themselves and all members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiffs seeks certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following Class:

> All persons in the United States whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

200. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which Defendant has a controlling interest, as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s).

201. Plaintiffs reserve the right to modify or amend the foregoing Class definition before the Court determines whether certification is appropriate.

202. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable.

203. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. These common questions of law or fact include, *inter alia*:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

c. Whether Defendant's computer systems and data security practices used to protect Plaintiffs' and Class Members' Private Information violated the FTC Act and/or state laws, and/or Defendant's other duties discussed herein;

d. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class Members;

e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

g. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Plaintiffs and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

i. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' Private Information;

j. Whether Defendant breached duties to protect Plaintiffs' and Class Members' Private Information;

k. Whether Defendant's actions and inactions alleged herein were negligent;

l. Whether Defendant were unjustly enriched by their conduct as alleged herein;

m. Whether an implied contract existed between Class Members and Defendant with respect to protecting Private Information and privacy, and whether that contract was breached;

n. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages or other relief, and the measure of such damages and relief;

o. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

p. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

204. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

205. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their Private Information compromised in the Data Breach. Plaintiffs and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

206. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs are adequate representatives of the Class and have no interests adverse to, or in conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial

experience and success in the prosecution of complex consumer protection class actions of this nature.

207. Superiority: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class Members to individually seek redress from Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

208. Injunctive and Declaratory Relief: Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

209. Likewise, particular issues are appropriate for certification under Rule 24(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to: (a) whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, and safeguarding their Private Information; (b) whether Defendant failed to adequately monitor and audit their data security systems; and (c) whether

Defendant failed to take reasonable steps to safeguard the Private Information of Plaintiffs and Class Members.

210. All members of the proposed Class are readily ascertainable. Defendant has access to the names in combination with addresses and/or e-mail addresses of Class Members affected by the Data Breach. Indeed, impacted Class Members already have been preliminarily identified and sent a breach notice letter.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

211. Plaintiffs hereby repeat and reallege paragraphs 1 through 210 of this Complaint and incorporate by reference herein.

212. Defendant requires its patients to submit non-public Private Information as a condition of receiving treatment.

213. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business, which affects commerce.

214. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that the information would be safeguarded.

215. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if their Private Information were wrongfully disclosed.

216. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

217. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

218. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiffs and Class Members, on the other hand. That special relationship arose because Defendant was entrusted with their confidential Private Information as a condition of receiving treatment from Defendant.

219. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information that was no longer required to be retained pursuant to regulations.

220. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach but failed to do so.

221. Defendant had and continues to have duties to adequately disclose that Plaintiffs' and Class Members' Private Information within Defendant's possession has been compromised, how it was compromised, and precisely the types of data that was compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

222. Defendant breached its duties and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

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

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

223. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

224. Defendant knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' Private Information would cause damage to Plaintiffs and the Class.

225. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures, caused the same harm as that suffered by Plaintiffs and the Class.

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

227. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach

of security was reasonably foreseeable given the known high frequency of corporate cyberattacks and data breaches.

228. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

229. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on its systems.

230. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

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

232. Defendant's duties extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

233. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

234. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiffs and the Class, Plaintiffs' and Class Members' Private Information would not have been compromised.

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

236. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by the Data Breach; (x) the value of the unauthorized access to their Private Information permitted by Defendant; and (xi) any nominal damages that may be awarded.

237. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses including nominal damages.

238. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

239. Defendant's negligent conduct is ongoing, in that it still possesses Plaintiffs' and Class Members' Private Information in an unsafe and insecure manner.

240. Plaintiff and Class Members are 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) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

241. Plaintiffs hereby repeat and reallege paragraphs 1 through 210 of this Complaint and incorporate by reference herein.

242. Defendant had duties arising under the FTC Act and HIPAA to protect Plaintiffs' and Class Members' Private Information.

243. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private

Information; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized access to Class Members' Private Information; (iv) failing to detect in a timely manner that Class Members' Private Information had been compromised; (v) failing to remove former patients' Private Information that Defendant was no longer required to retain pursuant to regulations; and (vi) failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

244. Defendant's violations of Section 5 of the FTC Act and HIPAA (and similar state statutes) constitute negligence *per se*.

245. Plaintiffs and Class Members are consumers within the class of persons that Section 5 of the FTC Act and HIPAA were intended to protect.

246. The harm that has occurred is the type of harm the FTC Act and HIPAA were intended to guard against.

247. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures, caused the same harm as that suffered by Plaintiff and the Class.

248. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

249. In addition, under state data security and consumer protection statutes such as those outlined herein, Defendant had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information.

250. Plaintiffs and Class Members were foreseeable victims of Defendant's violations of the FTC Act and HIPAA, and state data security and consumer protection statutes. Defendant knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class Members' Private Information would cause damage to Plaintiff and the Class.

251. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

252. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

253. Finally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized

disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

254. Plaintiffs hereby repeat and reallege paragraphs 1 through 210 of this Complaint and incorporate by reference herein.

255. When Plaintiffs and Class Members provided their Private Information to Defendant, Plaintiffs and Class Members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their data had been breached and compromised.

256. Defendant required Plaintiffs and Class Members to provide and entrust their Private Information as a condition of receiving treatment.

257. Plaintiffs and Class Members would not have provided and entrusted Private Information to Defendant in the absence of the implied contract between them and Defendant.

258. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

259. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect the Private Information of Plaintiffs and Class Members and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach.

260. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

261. Plaintiffs hereby repeat and reallege paragraphs 1 through 210 of this Complaint and incorporate by reference herein.

262. This count is brought in the alternative to Plaintiffs' breach of implied contract count.

263. Plaintiffs and Class Members conferred a benefit on Defendant by paying Defendant for services and providing Defendant their Private Information.

264. The monies paid to Defendant were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiffs and Class Members.

265. Defendant failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiffs and Class Members, and as a result Defendant was overpaid.

266. Under principles of equity and good conscience, Defendant should not be permitted to retain the money because Defendant failed to provide adequate safeguards and security measures to protect Plaintiffs and Class Members' Private Information that they paid for but did not receive.

267. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class Members.

268. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

269. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

270. Plaintiffs hereby repeat and reallege paragraphs 1 through 210 of this Complaint and incorporate by reference herein.

271. In providing their Private Information, directly or indirectly, to Defendant, Plaintiffs and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and class members to safeguard and keep confidential their Private Information.

272. Defendant accepted the special confidence Plaintiffs and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiffs' and Class Members' Private Information as detailed in its Privacy Policy.

273. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became a guardian of Plaintiffs' and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members, for the safeguarding of Plaintiffs' and Class Members' Private Information.

274. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of the medical provider-patient relationship, in particular, to keep secure the patients' Private Information.

275. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing

to protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

276. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

277. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

278. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Class)

279. Plaintiffs hereby repeat and reallege paragraphs 1 through 210 of this Complaint and incorporate by reference herein.

280. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential, novel, and sensitive nature of Plaintiffs' and the Class members' Private Information that Plaintiffs and Class Members provided to Defendant.

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

282. Plaintiffs and Class Members provided their respective Private Information to Defendant, directly or indirectly, with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

283. Plaintiffs and Class Members also provided their respective Private Information to Defendant with the explicit understanding that Defendant would take precautions to protect that Private Information from unauthorized disclosure, such as following basic principles of information security practices.

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

285. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiffs' and Class members' Private Information, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

286. But for Defendant's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, the Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties.

Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Private Information, as well as the resulting damages.

287. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private Information. Defendant knew or should have known its security systems were insufficient to protect the Private Information that is coveted by thieves worldwide. Defendant also failed to observe industry standard information security practices.

288. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class Members suffered damages as alleged above.

COUNT VII
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)

289. Plaintiffs hereby repeat and reallege paragraphs 1 through 210 of this Complaint and incorporate by reference herein.

290. Plaintiffs and the Class Members had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

291. Defendant owed a duty to its current and former patients, including Plaintiffs and the Class Members, to keep this information confidential.

292. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' Private Information is highly offensive to a reasonable person.

293. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and Class Members disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and

protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

294. The Data Breach constitutes an intentional interference with Plaintiffs and the Class Members in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

295. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

296. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and Class Members in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

297. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

298. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiffs and Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

299. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

300. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members since their Private Information is still maintained by Defendant with their inadequate cybersecurity system and policies.

301. Plaintiffs and Class Members have no adequate remedy at law for the injuries

relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and the Class.

302. In addition to injunctive relief, Plaintiff, on behalf of herself and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs

COUNT VIII
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

303. Plaintiffs hereby repeat and reallege paragraphs 1 through 210 of this Complaint and incorporate by reference herein.

304. 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. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

305. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs allege that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

306. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class members.

307. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

308. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

309. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs' and Class Members' injuries.

310. If an injunction is not issued, the resulting hardship to Plaintiffs and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the class, respectfully request that the Court enter judgment in Plaintiffs' favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, nominal damages and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the class, seek appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all claims herein so triable.

Dated: November 25, 2024. Respectfully submitted,

/s/Jeffrey S. Goldenberg
Jeffrey S. Goldenberg
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Tel: (513) 345-8291
jgoldenberg@gs-legal.com

Kenneth J. Grunfeld
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
E: grunfeld@kolawyers.com

Interim Co-Lead Class Counsel

Bret R. Cohen
LEEDS BROWN LAW, P.C.
One Old Country Road, Suite 347
Carle Place, NY 11514
Tel: (516) 873-9550
bcohen@leedsbrownlaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com

Andrew J. Shamis, Esq.
SHAMIS & GENTILE P.A.
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com

Counsel for Plaintiffs and Proposed Class

E-FILED
Monday, 25 November, 2024 01:38:53 PM
Clerk, U.S. District Court, ILCD

EXHIBIT A

Hospital Sisters
HEALTH SYSTEM

[redacted]

Dear Nick Glenn Avery:

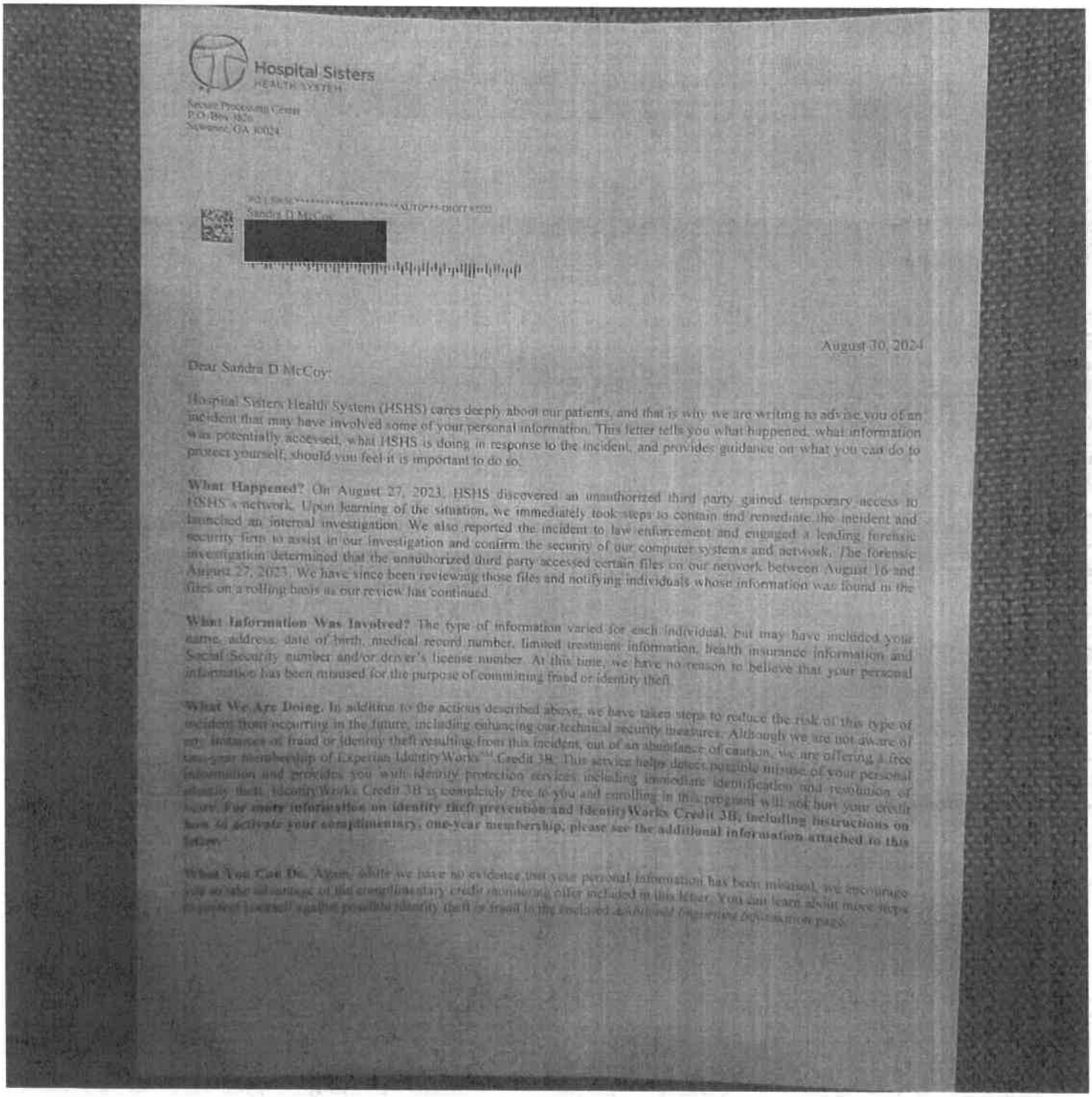
Hospital Sisters Health System (HSHS) cares deeply about our patients, and that is why we are writing to advise you of an incident that may have involved some of your personal information. This letter tells you what happened, what information was potentially accessed, what HSHS is doing in response to the incident, and provides guidance on what you can do to protect yourself, should you feel it is important to do so.

What Happened? On August 27, 2023, HSHS discovered an unauthorized third party gained temporary access to HSHS's network. Upon learning of the situation, we immediately took steps to contain and remediate the incident and launched an internal investigation. We also reported the incident to law enforcement and engaged a leading forensic security firm to assist in our investigation and confirm the security of our computer systems and network. The forensic investigation determined that the unauthorized third party accessed certain files on our network between August 16 and August 27, 2023. We have since been reviewing those files and notifying individuals whose information was found in the files on a rolling basis as our review has continued.

What Information Was Involved? The type of information varied for each individual, but may have included yo *name, address, date of birth, medical record number, limited treatment information, health insurance information Social Security number and/or driver's license number. At this time, we have no reason to believe that your pers information has been misused for the purpose of committing fraud or identity theft.*

What We Are Doing. *In addition to the actions described above, we have taken steps to reduce the risk of this t cident from occurring in the future, including enhancing our technical security measures. Although we are not a* y instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are offerin e-year membership of Experian IdentityWorks℠ Credit 3B. This service helps detect possible misuse of your formation and provides you with identity protection services including immediate identification and reso ntity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt y re. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instr v to activate your complimentary, one-year membership, please see the additional information attac er.**

t You Can Do. Again, while we have no evidence that your personal information has been misused, o take advantage of the complimentary credit monitoring offer included in this letter. You can learn ab otect yourself against possible identity theft or fraud in the enclosed *Additional Important Information*



Hospital Sisters
HEALTH SYSTEM

Secure Processing Center
P.O. Box 1626
Suwanee, GA 30024

[redacted]
Sandra D McCoy
[redacted]

August 30, 2024

Dear Sandra D McCoy:

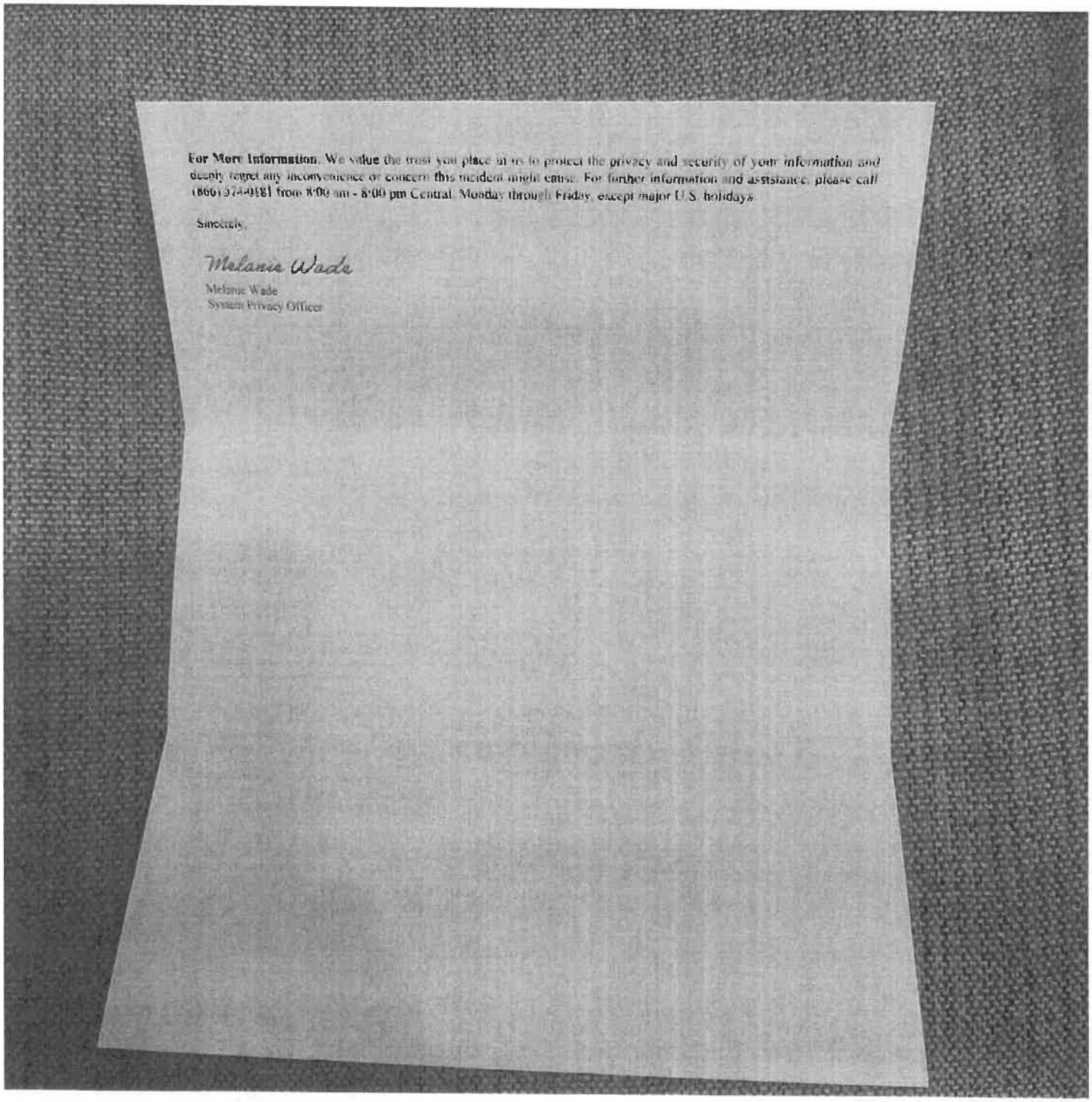
Hospital Sisters Health System (HSHS) cares deeply about our patients, and that is why we are writing to advise you of an incident that may have involved some of your personal information. This letter tells you what happened, what information was potentially accessed, what HSHS is doing in response to the incident, and provides guidance on what you can do to protect yourself, should you feel it is important to do so.

What Happened? On August 27, 2023, HSHS discovered an unauthorized third party gained temporary access to HSHS's network. Upon learning of the situation, we immediately took steps to contain and remediate the incident and launched an internal investigation. We also reported the incident to law enforcement and engaged a leading forensic security firm to assist in our investigation and confirm the security of our computer systems and network. The forensic investigation determined that the unauthorized third party accessed certain files on our network between August 16 and August 27, 2023. We have since been reviewing those files and notifying individuals whose information was found in the files on a rolling basis as our review has continued.

What Information Was Involved? The type of information varied for each individual, but may have included your name, address, date of birth, medical record number, limited treatment information, health insurance information and Social Security number and/or driver's license number. At this time, we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft.

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident from occurring in the future, including enhancing our technical security measures. Although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are offering a free one-year membership of Experian IdentityWorks℠ Credit 3B. This service helps detect possible misuse of your personal information and provides you with identity protection services including immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. Again, while we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring offer included in this letter. You can learn about more steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

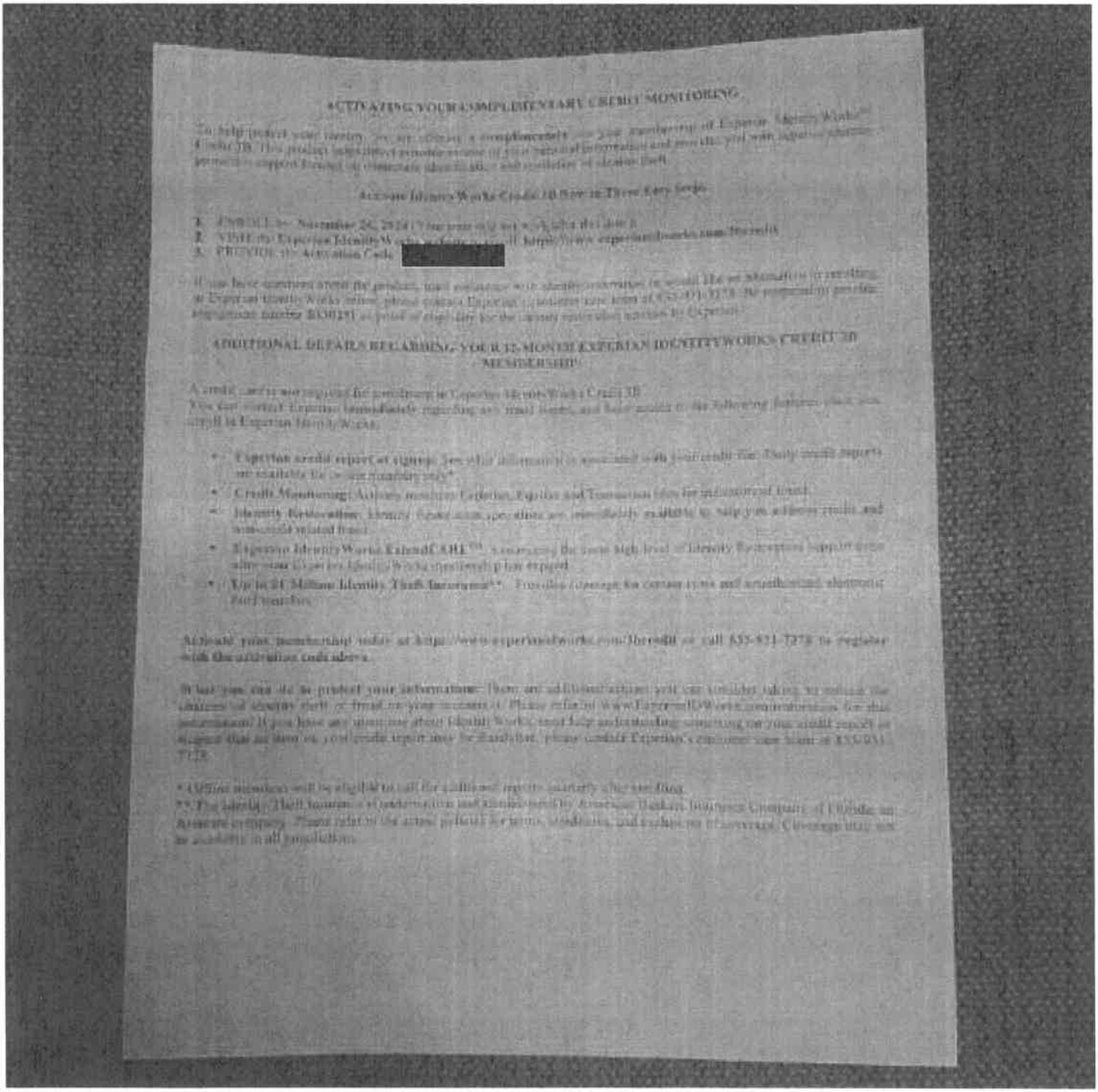


For More Information. We value the trust you place in us to protect the privacy and security of your information and deeply regret any inconvenience or concern this incident might cause. For further information and assistance, please call (866)574-0581 from 8:00 am - 5:00 pm Central, Monday through Friday, except major U.S. holidays.

Sincerely,

Melanie Wade

Melanie Wade
System Privacy Officer



ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: November 26, 2024 (Your code will not work after this date.)
2. VISIT the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
3. PROVIDE the Activation Code: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-7278. Be prepared to provide engagement number B130191 as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks Credit 3B.
You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only*.
- Credit Monitoring: Actively monitors Experian, Equifax and Transunion files for indications of fraud.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE™: You receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- Up to $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit or call 833-931-7278 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 833-931-7278.

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Hospital Sisters
HEALTH SYSTEM

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

3171 5233 ********** AUTO**5 DIGIT 62411
Charles R Bovard
[redacted]

August 30, 2024

Dear Charles R Bovard:

Hospital Sisters Health System (HSHS) cares deeply about our patients, and that is why we are writing to advise you of an incident that may have involved some of your personal information. This letter tells you what happened, what information was potentially accessed, what HSHS is doing in response to the incident, and provides guidance on what you can do to protect yourself, should you feel it is important to do so.

What Happened? On August 27, 2023, HSHS discovered an unauthorized third party gained temporary access to HSHS's network. Upon learning of the situation, we immediately took steps to contain and remediate the incident and launched an internal investigation. We also reported the incident to law enforcement and engaged a leading forensic security firm to assist in our investigation and confirm the security of our computer systems and network. The forensic investigation determined that the unauthorized third party accessed certain files on our network between August 16 and August 27, 2023. We have since been reviewing those files and notifying individuals whose information was found in the files on a rolling basis as our review has continued.

What Information Was Involved? The type of information varied for each individual, but may have included your name, address, date of birth, medical record number, limited treatment information, health insurance information and Social Security number and/or driver's license number. At this time, we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft.

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident from occurring in the future, including enhancing our technical security measures. Although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are offering a free one-year membership of Experian IdentityWorks℠ Credit 3B. This service helps detect possible misuse of your personal information and provides you with identity protection services including immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. Again, while we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring offer included in this letter. You can learn about more steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

For More Information. We value the trust you place in us to protect the privacy and security of your information and deeply regret any inconvenience or concern this incident might cause. For further information and assistance, please call (866) 574-0181 from 8:00 am - 8:00 pm Central, Monday through Friday, except major U.S. holidays.

Sincerely,

Melanie Wade

Melanie Wade
System Privacy Officer

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **November 26, 2024** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code:** [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-7378. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.
You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit or call 833-931-7378 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 833-931-7378.

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Hospital Sisters
HEALTH SYSTEM
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

677 I 110315 **********AUTO**5-DIGIT 62704
Kim Simone Wade
[redacted]

August 30, 2024

Dear Kim Simone Wade:

Hospital Sisters Health System (HSHS) cares deeply about our patients, and that is why we are writing to advise you of an incident that may have involved some of your personal information. This letter tells you what happened, what information was potentially accessed, what HSHS is doing in response to the incident, and provides guidance on what you can do to protect yourself, should you feel it is important to do so.

What Happened? On August 27, 2023, HSHS discovered an unauthorized third party gained temporary access to HSHS's network. Upon learning of the situation, we immediately took steps to contain and remediate the incident and launched an internal investigation. We also reported the incident to law enforcement and engaged a leading forensic security firm to assist in our investigation and confirm the security of our computer systems and network. The forensic investigation determined that the unauthorized third party accessed certain files on our network between August 16 and August 27, 2023. We have since been reviewing those files and notifying individuals whose information was found in the files on a rolling basis as our review has continued.

What Information Was Involved? The type of information varied for each individual, but may have included your name, address, date of birth, medical record number, limited treatment information, health insurance information and Social Security number and/or driver's license number. At this time, we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft.

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident from occurring in the future, including enhancing our technical security measures. Although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are offering a free one-year membership of Experian IdentityWorks℠ Credit 3B. This service helps detect possible misuse of your personal information and provides you with identity protection services including immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. Again, while we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring offer included in this letter. You can learn about more steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.