UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

BRIAN TROESCH, on behalf of themselves and all others similarly situated, Plaintiff, v. ABBOTT LABORATORIES, INC. and EXACT SCIENCES CORPORATION, Defendants.	Case No. _____ CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Brian Troesch ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this action against Abbott Laboratories, Inc. ("Abbott") and Exact Sciences Corporation ("Exact Sciences" and, together with Abbott, "Defendants"). Plaintiff brings this action by and through his attorneys, and alleges, based upon personal knowledge as to his own actions, and based upon information and belief and reasonable investigation by his counsel as to all other matters, as follows.

I. INTRODUCTION

1. Abbott is a multinational healthcare and medical-device company headquartered in Abbott Park, Illinois.

2. Exact Sciences is a clinical laboratory company that provides diagnostic testing and cancer screening services to patients and healthcare providers throughout the United States.

3. As part of their operations, Defendants collect, maintain, and store highly sensitive "personally identifying information" ("PII"), "private health information" ("PHI"), and "financial account information" from their patients (collectively "Private Information").

4. On or about July 15, 2026, cybercriminals attacked Defendants' systems, encrypting data and disrupting services. On information and belief, the cybercriminals also successfully stole vast quantities of sensitive Private Information maintained by Defendants (the "Breach" or "Data Breach").

5. On July 16, 2026, Abbott published a statement on its website indicating that it is "investigating a cyber incident."[1]

6. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief for, *inter alia*, the consequences of Defendants' failure to reasonably safeguard their Private Information; their failure to reasonably provide timely notification to Plaintiff and Class members that their Private Information had been compromised; and for Defendants' failure to inform Plaintiff and Class members concerning the status, safety, location, access, and protection of their Private Information.

II. PARTIES

Plaintiff Brian Troesch

7. Plaintiff Brian Troesch is a resident and citizen of Chicago, Illinois. Plaintiff Troesch was a patient at Exact Sciences. On information and belief, Plaintiff Troesch's Private Information was in Defendants' possession at the time of the Data Breach and accessed by the cybercriminals.

[1] https://www.abbott.com/en-us/corpnewsroom/diagnostics-testing/abbott-statement-on-cyber-incident-in-cancer-diagnostics-business (last visited July 22, 2026).

Defendant Abbott Laboratories, Inc.

8. Defendant Abbott Laboratories, Inc. is a corporation headquartered at 100 Abbott Park Road, Abbott Park, Illinois, 60064.

Defendant Exact Sciences Corporation

9. Defendant Exact Sciences Corporation is a Delaware corporation headquartered at 5505 Endeavor Lane, Madison, WI 53719. Defendant conducts business in Illinois.

III. JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, namely Plaintiff, a citizen of Illinois, is a citizen of a state different from Exact Sciences.

11. This Court has personal jurisdiction over Defendants because Abbott's principal place of business is in this District, Defendants regularly conduct business in this District, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

12. Venue is proper under 18 U.S.C § 1391(b)(1) because Abbott's principal place of business is in this District and a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Defendants' Backgrounds

13. Abbott is a multinational healthcare and medical device company headquartered in Abbott Park, Illinois.

14. Exact Sciences is a clinical laboratory and molecular diagnostics company that offers a variety of cancer screening, diagnostic testing, and related laboratory services to patients

and healthcare providers throughout the United States. In the course of providing these services, Exact Sciences collects, stores, and maintains sensitive PII and PHI entrusted to them by patients.

15. As healthcare services providers, Defendants collect, maintain, and store large volumes of Private Information belonging to their current and former patients as part of their general business operations.

16. Upon information and belief, Defendants failed to implement necessary data security safeguards at the time of the Data Breach. On information and belief, this failure resulted in cybercriminals accessing the Private Information of Defendants' current and former patients—Plaintiff and Class members.

17. Current and former patients of Defendants, such as Plaintiff and Class members, made their Private Information available to Defendants with the reasonable expectation that any entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. They similarly expected that, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

18. This expectation was objectively reasonable and based on an obligation imposed on Exact Sciences by statute, regulations, industrial custom, and standards of general due care.

19. Had they known that Defendants' systems were vulnerable and open to attack, Plaintiff and Class members, as reasonable individuals, would not have provided their Private Information to Defendants; instead, they would have sought out a competitor for their healthcare needs.

20. Unfortunately for Plaintiff and Class members, Defendants failed to carry out their duty to safeguard sensitive Private Information and provide adequate data security. As a result,

they failed to protect Plaintiff and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

21. On or about July 15, 2026, public reports indicated that a ransomware group claimed responsibility for a cyberattack targeting Defendants' information systems. Since the Data Breach, notorious ransomware group "Shinyhunters" claimed responsibility.[2]

22. Shunyhunters is a notorious black-hat cybercriminal group that specializes in large-scale data breaches, extortion, and selling stolen user data on the dark web.[3]

23. On information and belief, Shinyhunters accessed and obtained current and former patients' Private Information during the Data Breach, as is the *modus operandi* of cybercriminals in these types of data incidents.

C. Defendants' Many Failures Both Prior to and Following the Breach

24. The Data Breach and the injuries it caused to Plaintiff and Class members occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendants.

25. First, Defendants inexcusably failed to implement reasonable security protections to safeguard their information systems and databases.

26. Second, Defendants failed to inform the public that their data security practices were deficient and inadequate. Had Plaintiff and Class members been aware that Defendants did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Defendants.

[2] https://www.hendryadrian.com/ransom-abbott-owned-exact-sciences-corporation-jul-2026/ (last visited July 22, 2026).
[3] https://www.docontrol.io/blog/shinyhunters (last visited July 22, 2026).

27. To date, Defendants have not yet provided direct notice to individuals whose Private Information was accessed in the Data Breach.

D. Data Breaches Are Prevalent

28. While the prevalence and severity of data breaches have increased exponentially over the past five years, the illicit trade of stolen data dates back to the earliest days of the internet. In the 1990s, cybercriminals sold stolen data through Internet Relay Chat (IRC) channels, which were primitive message boards and instant messaging services, before transitioning to dedicated web forums in the early 2000s.[4] These forums became havens for cybercriminals of all stripes where "individuals advertised their services to other users. Forums quickly gained popularity and became successful businesses with vendors selling stolen credit cards, malware, and related goods and services to misuse personal information and enable fraud."[5]

29. A forum known as ShadowCrew, which operated for just two years before being shut down by a law enforcement task force operation in 2004, served as the most prominent port of call during this era, and its members managed to traffic over 1.7 million stolen credit card details in the brief period of time it was online.[6]

30. The end of ShadowCrew did not dampen the illicit trade in stolen data. Instead, the trade moved to the dark web where it thrives to this day. Gone are the days of archaic IRC channels and dusty forums; stolen data is now traded on dedicated webpages serving as veritable e-commerce stores (akin to Amazon, eBay, and Alibaba) for stolen data of all kinds, complete with

[4] Thomas Holt, *How massive data breaches flood illicit markets while personal information fuels cybercrime economy*, Milwaukee Independent (November 12, 2025), available at https://www.milwaukeeindependent.com/syndicated/massive-data-breaches-flood-illicit-markets-personal-information-fuels-cybercrime-economy/.
[5] *Id.*
[6] *Id.*

eye-catching webpages, distinct branding, and advertising to attract customers.[7] The vendors operating from these dark web storefronts are "frequently offer discounts and promotions to buyers to attract customers and keep them loyal," and offer clearance sales on old and/or expiring inventory, such as expiring credit card numbers, in a macabre reflection of commercial practices from the right side of the law.[8]

31. This decades-old black market for stolen data continues to thrive, and stolen PII, PHI, and financial account information are exchanged as simple commodities with prices set by the brutal and invisible hand of economics. Typically, online banking login information can be purchased for $100 each, full credit card details can be purchased for between $10 and $100, and comprehensive data packages which can enable complete theft of an individual's identity can be purchased for $1,000 or more.[9]

32. For criminals, the ROI on purchased information can be exceptional despite the dubious nature of black-market dealings and the inherent risks therein. For example, a cybercriminal "who buys 100 cards for $500 can recoup costs if only 20 of those cards are active and can be used to make an average purchase of $30."[10] Based on these incentives, data breaches "are likely to continue as long as there is demand for illicit, profitable data."[11]

33. In this thriving black market, the producers are the cybercriminals who steal information to sell. And fueled by the voracious demand for stolen data in this thriving black

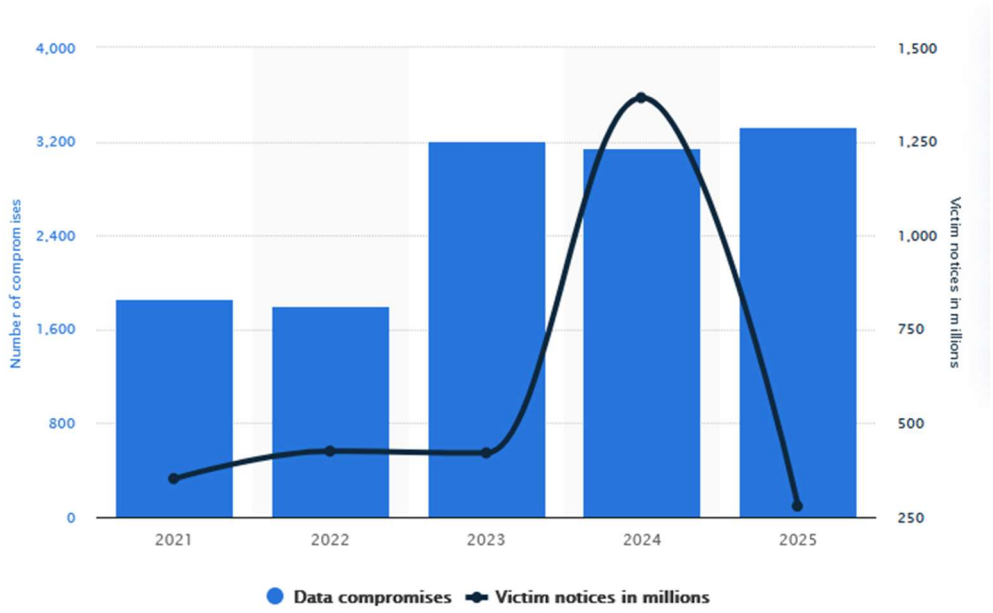
---

[7] *Id.*
[8] *Id.*
[9] Ryan Smith, *Revealed-how much is personal information worth on the dark web?*, Insurance News (May 1, 2023), available at https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx.
[10] Thomas Holt, *How massive data breaches flood illicit markets while personal information fuels cybercrime economy*, Milwaukee Independent (November 12, 2025), available at https://www.milwaukeeindependent.com/syndicated/massive-data-breaches-flood-illicit-markets-personal-information-fuels-cybercrime-economy/.
[11] *Id.*

market, dedicated gangs and organized crime rings have stepped up to meet the market demand, which has resulted in a precipitous increase in the number of data breaches in recent years.

34. The Identity Theft Resource Center's ("ITRC") Annual End-of-Year Data Breach Report for 2025 listed 3,322 data breach incidents which occurred in 2025, for which 232,726,796 individual victim notices were dispatched.[12] Indeed, 2025 handily dethroned 2023 as the most prolific year for data breaches, which previously held the title with 3,205 data breaches for which over 420 million individual victim notices were dispatched.[13]

35. Data breaches show no sign of abating. Statista, a German entity that collects and markets data relating to, *inter alia*, data breach incidents and the consequences thereof, reported 3,322 data breach incidents in the United States in 2025, 3,152 data breach incidents in 2024, 3,205 incidents in 2023, and 1,798 incidents in 2022.[14]



[12] *2025 Data Breach Report*, Identity Theft Resource Center (January 2026), available at https://www.idtheftcenter.org/publication/2025-data-breach-report/.
[13] *Id.*
[14] *Number of data compromises and individuals impacted in the United States from 2021 to 2025*, Statista (February 15, 2026), available at https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

Figure 1 – *Number of Data Breaches and Affected Individuals from 2005 to 2024.*[15]

E. How the Theft and Sale of Data Harms Victims and Organizations

36. Individuals who have unfortunately had their information stolen and sold on the black-market face severe consequences which belie the blatant ubiquity of such transactions. According to a recent study published in the scholarly journal *Preventive Medicine Reports*, public and corporate data breaches strongly correlate to an increased risk of identity theft for victimized consumers, with one in four victims of a data breach inevitably experiencing some type of identity theft.[16]

37. Using this stolen information, criminals and other unsavory groups can fraudulently take out loans under the victims' names, open new lines of credit, open new bank accounts for purposes of committing fraud, and file fraudulent tax returns using stolen credentials.[17]

38. Victims can even face criminal charges as a result of identity theft and typically experience significant emotional distress:

> Having your identity stolen can be traumatic. Nearly 9 in 10 respondents (87%) in the ITRC survey reported feeling anxious or worried in the wake of identity theft; 77% felt violated, and an alarming 16% reported feeling suicidal in the months following identity theft. Identity theft victims report feeling unable to trust friends (34%) and family members (33%). More than half (52%) say they feel embarrassed or ashamed, even though ID theft can be difficult for the average person to detect and thwart, and some forms of identity theft, such as data breaches, are beyond the victims' control. Shame, suspicion and a feeling you should be curtailing your activity to prevent further theft can lead to isolation.[18]

---

[15] *Id.*

[16] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.

[17] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[18] Gayle Sato, What Are the Unexpected Costs of Identity Theft? Experian (July 30, 2024), available at https://www.experian.com/blogs/ask-experian/what-are-unexpected-costs-of-identity-theft/.

39. These difficulties compound when Social Security numbers are compromised in the Breach. A victim is forbidden from proactively changing his or her number unless and until they can prove actual misuse and harm, and even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[19]

40. The consequences of identity theft do not resolve quickly. In a survey of identity theft victims conducted by the Identity Theft Research Center (ITRC), 77% of respondents reported having at least some financial problems following identity theft, with 61% saying they had difficulty covering basic needs. Although 28% said they resolved their issues within six months of an ID theft incident, 65% said issues remained unresolved even after a year.[20]

41. On average, victims of identity theft spend $1,200 to restore their identity and resolve damage to their credit, which includes payments to specialists and attorneys and lost wages.[21]

42. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[22] The average cost to resolve a

---

[19] *Id.*
[20] *Id.*
[21] Alexandria White and Dan Avery, What is identity theft insurance? CNBC Select (March 17, 2025), available at https://www.cnbc.com/select/id-theft-insurance/#:~:text=Victims%20of%20identity%20theft%20spend,lost%20wages%20and%20other%20expenses.
[22] *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.

data breach involving health information, however, is more than double this figure at $10.92 million.[23]

43. Furthermore, even if only a select few categories of Private Information is compromised in a breach, cybercriminals can use these pieces of stolen information to create a "mosaic" of information on each victim. In effect, cybercriminals can use the information stolen in one breach and connect it to other available information on the victims, which are data-mined from publicly available sources or illegally obtained from other breaches. Thus, even if certain categories of information such as emails, phone numbers, or credit card information were not compromised in this Data Breach, criminals can easily 'fill in the blanks' using these "mosaics" and correctly answer security questions and pass 2FA security checks, granting them access to victims' email accounts, financial accounts, and social media accounts to cause havoc.

44. A particularly troubling extension of these "mosaics" is the creation of "Fullz" packages. A "Fullz" package is a comprehensive dossier of information that cybercriminals compile on individuals, often through the use of automated programs, which represents an alarmingly accurate and complete profile of a given individual. These "Fullz" packages are sold for profit on the dark web to any individual willing and able to pay the price, be they cybercriminals seeking to perpetuate financial crimes, stalkers seeking information on their targets, or rivals seeking to destroy someone's reputation.

45. Upon information and belief, this has already transpired (and will continue to transpire) for Plaintiff and the Class. And any reasonable for any trier of fact will find that Plaintiff's and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach. There is also a high likelihood that significant identity

[23] *Id.*

fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

F. The Unique Severity of Medical Data Breaches

46. Much like standard data breaches, data breaches involving medical information is also pervasive. The HIPAA Journal's 2025 Health Care Data Breach Report noted 710 data breaches involving 500 or more healthcare records, though the HIPAA Journal believes this is greatly understated due to the effects of the prolonged government shutdown.[24] Indeed, Medical identity theft has seen a seven-fold increase over the last five years and this explosive growth far outstrips the increase in incidence of traditional identity theft.[25]

47. Stolen medical records are some of the most sought after and expensive commodities on the dark web, commanding prices from $250 to $1,000 each.[26] Medical records are considered valuable because unlike credit cards, which can easily be canceled, and social security numbers, which can be changed, medical records contain "a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information."[27] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims'

---

[24] Steve Adler, *2025 Healthcare Data Breach Report, The HIPAA Journal* (February 13, 2026), available at https://www.hipaajournal.com/2025-healthcare-data-breach-report/; The HIPAA Journal bases its numbers on the medical data breaches reported to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR). The OCR makes these reports publicly available; however, the HIPAA Journal believes OCR has been experiencing delays in processing and publicizing its reports due to the government shutdown.

[25] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.

[26] Paul Nadrag, *Capsule Technologies, Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (January 26, 2021), available at: https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

[27] *Id.*

accounts.[28] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[29] Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[30]

48. The wrongful use of compromised medical information, known as medical identity theft, is far more harmful than standard identity theft. Victims of medical identity theft spend an average of $13,500 to resolve the consequences, and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[31] It is also "considerably harder" to reverse the damage from the typical consequences of medical identity theft.[32]

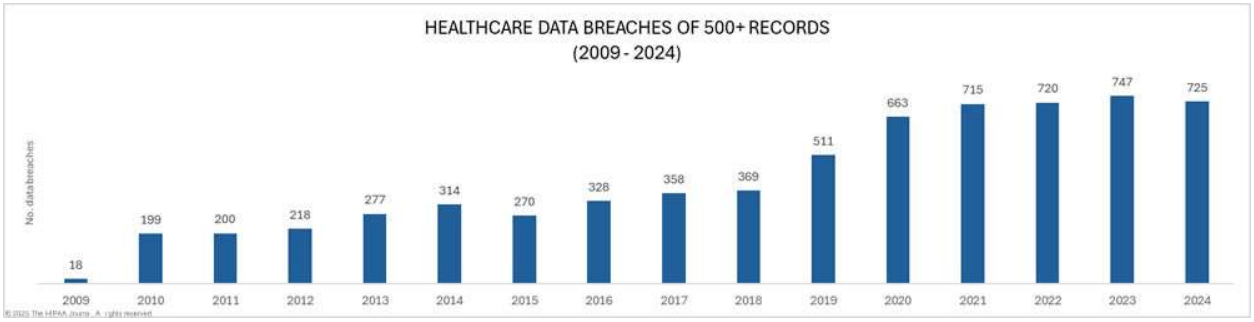


Figure 2 – *Number of Individuals Affected by Healthcare Data Breaches from 2009 to 2024.*[33]

[28] *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), available at https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare. *See also* Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (August 25, 2016), available at https://www.consumerreports.org/health/medical-identity-theft-a1699327549/; *Data Breaches: In the Healthcare Sector*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited December 1, 2024).
[29] *Id.*
[30] *Id.*
[31] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.
[32] *Id.*
[33] Steve Adler, 2024 Healthcare Data Breach Report, The HIPAA Journal (January 30, 2025), available at https://www.hipaajournal.com/december-2023-healthcare-data-breach-report/.

49. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities charged with maintaining and securing patient PII, such as Defendants, should know the importance of protecting that information from unauthorized disclosure. Indeed, Defendants knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[34]

50. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendants on notice of their obligation to safeguard customer and patient information.[35]

51. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[36] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

---

[34] *See, e.g.*, Steve Adler, *Healthcare Data Breach Statistics*, HIPAA Journal (November 25, 2024), available at: https://www.hipaajournal.com/healthcare-data-breach-statistics.
[35] *See, e.g.*, *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).
[36] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. *See also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

52. Given the nature of the Data Breach, as well as the length of the time Defendants' networks were breached and the long delay in notification to victims thereof, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways.

53. Despite the prevalence of public announcements of data breach and data security compromises, their own acknowledgment of the risks posed by data breaches, and their own acknowledgment of their duties to keep Private Information private and secure, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from misappropriation. As a result, the injuries to Plaintiff and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for their current and former patients.

G. Defendants Had a Duty and Obligation to Protect Private Information

54. Defendants have an obligation to protect the Private Information belonging to Plaintiff and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and medical records. Third, Defendants imposed such an obligation on itself with their promises regarding the safe handling of data. Plaintiff and Class members provided, and Defendants obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. HIPAA Requirements and Violation

55. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably

anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq*.

56. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . . ." 45 CFR § 164.402.

57. Defendants failed to implement and/or maintain procedures, systems, and safeguards to protect the Private Information belonging to Plaintiff and Class members from unauthorized access and disclosure.

58. Upon information and belief, Defendants' security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1);

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

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforces, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

59. Upon information and belief, Defendants also failed to store the information they collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

2. FTC Act Requirements and Violations

60. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

61. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[37] The guidelines note businesses should protect the personal information

[37] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n

that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[38] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[39] Defendants clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

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

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

64. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

(October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed August 15, 2023).

[38] *Id.*

[39] *Id.*

65. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

66. Defendants were fully aware of their obligation to protect the Private Information of their current and former patients, including Plaintiff and Class members. Defendants are a sophisticated and technologically savvy businesses that rely extensively on technology systems and networks to maintain their practice, including storing their patients' PII, protected health information, and medical information, in order to operate their business.

67. Defendants had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendants and Plaintiff and Class members. Defendants alone had the exclusive ability to implement adequate security measures to their cyber security network to secure and protect Plaintiff's and Class members' Private Information.

3. Industry Standards and Noncompliance

68. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

69. Experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

70. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[40]

71. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

72. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks,

[40] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited Feb. 11, 2026).

including: (i) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (ii) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (iii) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[41]

73. Defendants failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

74. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

[41] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Feb. 11, 2026).

4. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

75. Like any data hack, the Data Breach presents major problems for all affected.[42] As discussed in detail above, Plaintiff and the Class are highly likely to experience identity theft and medical identity theft as a result of the Data Breach and, as also discussed in detail above, they are highly likely to experience significant harm as a result.

76. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with time spent to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendants' delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiff's and Class members' privacy.

[42] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.

77. As a direct and proximate result of Defendants' acts and omissions in failing to protect and secure Private Information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and they have incurred and will incur actual damages in an attempt to prevent identity theft.

78. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both himself and similarly situated individuals whose Private Information was accessed in the Data Breach.

G. EXPERIENCES SPECIFIC TO PLAINTIFF

Plaintiff Troesch

79. Plaintiff Troesch is a patient of Defendants.

80. On information and belief, Plaintiff's Private Information was in Defendants' possession at the time of the Data Breach, and was improperly accessed and obtained by third parties.

81. As a result of the Data Breach, Plaintiff Troesch has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Troesch has also spent several hours dealing with the Data Breach, valuable time Plaintiff Troesch otherwise would have spent on other activities, including, but not limited to, work and recreation.

82. As a result of the Data Breach, Plaintiff Troesch has suffered anxiety due to the public dissemination of Plaintiff Troesch's personal information, which Plaintiff Troesch believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using Troesch's Private Information for purposes of identity theft and

fraud. Plaintiff Troesch is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

83. Plaintiff Troesch suffered actual injury from having Plaintiff Troesch's Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Plaintiff Troesch's Private Information, a form of property that Defendants obtained from him; (b) violation of Plaintiff Troesch's privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

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

V. CLASS REPRESENTATION ALLEGATIONS

85. Plaintiff brings this action on behalf of himself and, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, a Class of:

All persons whose Private Information was accessed in the Data Breach.

Excluded from the Class are Defendants, their executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

86. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

87. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendants and obtainable by Plaintiff only through the discovery process. On information and belief, the number

of affected individuals estimated to be tens of thousands. The members of the Class will be identifiable through information and records in Defendants' possession, custody, and control.

88. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Defendants learned of the Data Breach;

b. Whether hackers obtained Class members' Private Information via the Data Breach;

c. Whether Defendants' response to the Data Breach was adequate;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

f. Whether Defendants owed a duty to safeguard their Private Information;

g. Whether Defendants breached their duty to safeguard Private Information;

h. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

i. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;

j. Whether Defendants' conduct violated the FTCA and/or HIPAA;

k. Whether Defendants' conduct was negligent;

l. Whether Defendants' conduct was *per se* negligent;

m. Whether Defendants were unjustly enriched;

n. What damages Plaintiff and Class members suffered as a result of Defendants' misconduct;

o. Whether Plaintiff and Class members are entitled to actual and/or statutory damages; and

p. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief.

89. Typicality: Plaintiff's claims are typical of the claims of the Class as Plaintiff and all members of the Class had their Private Information compromised in the Data Breach. Plaintiff's claims and damages are also typical of the Class because they resulted from Defendants' uniform wrongful conduct. Likewise, the relief to which Plaintiff is entitled to is typical of the Class because Defendants have acted, and refused to act, on grounds generally applicable to the Class.

90. Adequacy: Plaintiff is an adequate class representative because his interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, he has retained counsel competent and highly experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously. Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor his counsel have any interests that are antagonistic to the interests of other members of the Class.

91. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class, a class action is superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action

device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendants' records and databases.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(By Plaintiff on behalf of the Class)

92. Plaintiff incorporates and realleges all allegations in Paragraphs 1 through 91 as if fully set forth herein.

93. Defendants owe a duty of care to protect the Private Information belonging to Plaintiff and Class members. Defendants also owe several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in their possession;

b. to protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in their possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class members pursuant to the FTCA;

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. to promptly notify Plaintiff and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

94. Defendants also owe this duty because they had a special relationship with Plaintiff's and Class members. Plaintiff and Class members entrusted their Private Information to Defendants on the understanding that adequate security precautions would be taken to protect this

information. Furthermore, only Defendants had the ability to protect their systems and the Private Information stored on them from attack.

95. Defendants also owe this duty because industry standards mandate that Defendants protect their patients' confidential Private Information.

96. Defendants also owe a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiff and Class members. This duty exists to provide Plaintiff and Class members with the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

97. Defendants breached the duties they owed to Plaintiff and Class members by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard their Private Information.

98. Defendants also breached the duties they owed to Plaintiff and Class members by failing to timely and accurately disclose that their Private Information had been improperly acquired and/or accessed.

99. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; and
- Permanently increased risk of identity theft.

100. Plaintiff and Class members were foreseeable victims of any inadequate security practices on the part of Defendants and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

101. In failing to provide prompt and adequate individual notice of the Data Breach, Defendants also acted with reckless disregard for the rights of Plaintiff and Class members.

102. Plaintiff and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT II
NEGLIGENCE *PER SE*
(By Plaintiff on behalf of the Class)

103. Plaintiff incorporates and realleges all allegations in Paragraphs 1 through 91 as if fully set forth herein.

104. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, imposes a duty on Defendants to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiff and Class members.

105. HIPAA imposes a duty on Defendants to implement reasonable safeguards to protect Plaintiff's and Class members' Private Information. 42 U.S.C. § 1302(d), *et seq*.

106. HIPAA also requires Defendants to render unusable, unreadable, or indecipherable all Private Information they collected. Defendants were required to do so through "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

107. Defendants violated the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiff's and Class members' Private Information.

108. Defendants violated HIPAA by failing to properly encrypt the Private Information they collected.

109. Defendants' failure to comply with HIPAA and the FTCA constitutes negligence *per se*.

110. Plaintiff and Class members are within the class of persons that the FTCA and HIPAA are intended to protect.

111. The relevant portions of the FTCA and HIPAA inform Defendants' duties, particularly with regard to Defendants' duty to protect Private Information in their possession.

112. It was reasonably foreseeable that Defendants' breach of their duties, by failing to protect and secure Plaintiff's and Class members' Private Information in compliance with the FTCA and HIPAA standards, would result in that information being accessed and stolen by unauthorized actors and cybercriminals.

113. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

114. Plaintiff and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems

and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(By Plaintiff on behalf of the Class)

115. Plaintiff incorporates and realleges all allegations in Paragraphs 1 through 91 as if fully set forth herein.

116. Plaintiff and Class members provided Defendants with their Private Information as an integral and necessary part of receiving medical services. Plaintiff and the Class also provided payment to Defendants in exchange for receiving medical services.

117. During the transaction of medical services for payment, Plaintiff and the Class, on one hand, and Defendants, on the other hand, entered into implied-in-fact contracts which included a provision that Defendants would safeguard and protect the confidentiality of Private Information belonging to Plaintiff and the Class. In effect, Defendants agreed to provide reasonable and adequate data security to Private Information in their possession.

118. The terms of these implied contracts, including the provision requiring Defendants to maintain reasonable data security measures, are described in federal laws, state laws, and industry standards, as alleged above. In addition, Defendants expressly adopted and assented to these terms in their public statements, representations, and promises as described above.

119. The implied contracts for data security also obligated Defendants to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information, as is consistent with industry custom and statutory requirements.

120. Defendants breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' Private Information; and by failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

121. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiff and Class members have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information. Thus, Plaintiff and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT IV
UNJUST ENRICHMENT
(By Plaintiff on behalf of the Class)

122. Plaintiff incorporates and realleges all allegations in Paragraphs 1 through 91 as if fully set forth herein.

123. This count is brought in the alternative to Count III.

124. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendants.

125. Plaintiff and the Class conferred payment to Defendants in exchange for medical services, and as an integral part of this transaction also conferred their Private Information to Defendants.

126. Plaintiff and Class members conferred their payment and Private Information with the understanding that a portion of the payment would be used to implement data security sufficient to adequately protect their Private Information. As such, a portion of the conferred payment represented a benefit that was to be used for a specific purpose.

127. Defendants were directly benefitted by the payments they received from Plaintiff and Class members, as these payments represented revenue that they used for business purposes and financial gain. As alleged above Defendants knew, or should have known, that they was supposed to spend a portion of their revenues on adequate data security measures to prevent the theft or compromise of Private Information.

128. However, upon information and belief, Defendants did not spend that portion of their revenues on adequate data security measures such as employee training, operation protocols, and firewalls, that would have prevented the Data Breach. Instead, upon information and belief, they opted for cheaper and inadequate data security measures and elected to increase their profits instead. Thus, Defendants knowingly and opportunistically elected to increase their own profits at the expense of Plaintiff and Class members.

129. By refusing to spend on data security the part of the payment that was conferred with that express purpose, Defendants knowingly and deliberately enriched themselves at the expense of Plaintiff and Class members. This represents an inequitable, unfair, and unconscionable practice and state of affairs.

130. Under the common law doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain their engorged profits which they unfairly and unconscionably gained at the expense of Plaintiff and Class members.

131. Defendants are therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically the enhanced profits Defendants gained by not implementing and adopting reasonable data security measures that would have prevented the Data Breach. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct.

COUNT V
BREACH OF FIDUCIARY DUTY
(By Plaintiff on behalf of the Class)

132. Plaintiff incorporates and realleges all allegations in Paragraphs 1 through 91 as if fully set forth herein.

133. Plaintiff brings this claim on behalf of himself and the Class.

134. Defendants have a fiduciary relationship with Plaintiff and Class members because they have a doctor-patient relationship.

135. Alternatively, Plaintiff and Class members provided their Private Information to Defendants in confidence with the reasonable belief that Defendants would protect their information. And in collecting and maintaining this Private Information, Defendants created a fiduciary relationship between them and Plaintiff and Class members.

136. As Defendants have a fiduciary relationship with Plaintiff and Class members, Defendants owe a duty to *primarily* act for the benefit of Plaintiff and Class members within the scope of their relationship. This included a duty to protect Plaintiff's and Class Members' Private Information.

137. These fiduciary duties and responsibilities are also described under the procedures set forth in the HIPAA Privacy Rule, including the procedures and definitions found in 45 C.F.R. §160.103 and 45 C.F.R. §164.530, which requires Defendants to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient information and to secure the health care information they maintain and to keep it free from disclosure.

138. Defendants breached these fiduciary duties by failing to implement adequate safeguards and causing Plaintiff's and Class members' Private Information to be disclosed to unauthorized third parties.

139. As a direct and proximate result of Defendants' breaches of their fiduciary duties and the resulting disclosure of Plaintiff and Class member's Private Information, Plaintiff and Class members have suffered damages, including, but not limited to exposure to heightened future risk of identity theft, loss of privacy, confidentiality, and emotional distress, and humiliation.

140. Thus, Plaintiff and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT VI
INVASION OF PRIVACY
(By Plaintiff on behalf of the Class)

141. Plaintiff incorporates and realleges all allegations in Paragraphs 1 through 91 as if fully set forth herein.

142. Plaintiff and Class members had a reasonable expectation of privacy in the Private Information that Defendants possessed and/or continues to possess.

143. By failing to keep Plaintiff's and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendants invaded Plaintiff's and Class members' privacy by:

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

b. Publicizing private facts about Plaintiff and Class members, which is highly offensive to a reasonable person.

144. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider Defendants' actions highly offensive.

145. Defendants invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

146. As a proximate result of such misuse and disclosures, Plaintiff's and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

147. In failing to protect Plaintiff's and Class members' Private Information, and in misusing and/or disclosing their Private Information, Defendants have acted with malice and oppression and in conscious disregard of Plaintiff's and Class members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing their own economic, corporate, and legal interests above the privacy interests of their patients. Plaintiff, therefore, seeks an award of damages, including punitive damages, on behalf of himself and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and Class members compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court award Plaintiff and Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

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

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

G. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

H. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the putative Class, demands a trial by jury on all issues so triable.

Date: July 22, 2026

Respectfully Submitted,

/s/ Nickolas J. Hagman

Nickolas J. Hagman
Henry V. Melville
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
nhagman@caffertyclobes.com
hmelville@caffertyclobes.com

LAUKAITIS LAW LLC
Kevin Laukaitis*
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Attorneys for Plaintiff and the Proposed Class

JS 44 (Rev. 03/24)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

BRIAN TROESCH, individually and on behalf of all others similarly situated;

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Nickolas J. Hagman, CAFFERTY CLOBES MERIWETHER & SPENGEL, LLP, 135 S. LaSalle, Suite

DEFENDANTS

ABBOTT LABORATORIES, INC. and EXACT SCIENCES CORPORATION

County of Residence of First Listed Defendant Dane County
(IN U.S. PLAINTIFF CASES ONLY)

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

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☑ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		INTELLECTUAL PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	☐ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☐ 370 Other Fraud	☐ 710 Fair Labor Standards Act	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 720 Labor/Management Relations	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 740 Railway Labor Act	☐ 880 Defend Trade Secrets Act of 2016	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 751 Family and Medical Leave Act	SOCIAL SECURITY	☐ 480 Consumer Credit (15 USC 1681 or 1692)
☐ 190 Other Contract	☑ 360 Other Personal Injury		☐ 790 Other Labor Litigation	☐ 861 HIA (1395ff)	☐ 485 Telephone Consumer Protection Act
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 791 Employee Retirement Income Security Act	☐ 862 Black Lung (923)	☐ 490 Cable/Sat TV
☐ 196 Franchise				☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
				☐ 864 SSID Title XVI	☐ 890 Other Statutory Actions
				☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
					☐ 893 Environmental Matters
				FEDERAL TAX SUITS	☐ 895 Freedom of Information Act
				☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 896 Arbitration
				☐ 871 IRS—Third Party 26 USC 7609	☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
					☐ 950 Constitutionality of State Statutes

REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	**Habeas Corpus:**	☐ 462 Naturalization Application
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee	☐ 465 Other Immigration Actions
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence	
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General	
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty	
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	**Other:**	
	☐ 448 Education	☐ 540 Mandamus & Other	
		☐ 550 Civil Rights	
		☐ 555 Prison Condition	
		☐ 560 Civil Detainee - Conditions of Confinement	

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
U.S.C. Sec. 1332(d)(2)

Brief description of cause:
Defendant suffered a data breach, which damaged a class of individuals whose personal information was stolen.

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☑ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
07/22/2026

SIGNATURE OF ATTORNEY OF RECORD
/s/ Nickolas J. Hagman

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

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

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

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

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

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

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

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

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

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

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

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

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