IN THE COURT OF COMMON PLEAS
OF LACKAWANNA COUNTY, PENNSYLVANIA

LAUREN M. MAILEN
LACKAWANNA COUNTY
2025 OCT -6 A 9:19
CLERK OF JUDICIAL RECORDS
CIVIL DIVISION

LEO WOYTACH, JAMES DAVIS, SHAWN TOOLAN, BRYCE ALLEN, SCOTT STOLARIK, CHAD MARTIN, HELENA JOHNSTON, JOE CLEMENTE, and HILARY BURNS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

DRUG AND ALCOHOL TREATMENT SERVICES, INC.,

Defendant.

Case No.: 2025-CV-03681

CONSOLIDATED AMENDED COMPLAINT – CLASS ACTION

JURY TRIAL DEMANDED

NOTICE

You have been sued in court. If you wish to defend against the claims set forth in the following pages you must take action within twenty (20) days after this complaint and notice are served by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE GO TO OR TELEPHONE THE OFFICES SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP.

NORTHEASTERN PENNSYLVANIA LEGAL SERVICES
33 N. MAIN STREET, SUITE 200
PITTSTON, PA 18640
TELEPHONE (570) 299-4100

Plaintiffs Leo Woytach, Shawn Toolan, James Davis, Bryce Allen Scott Stolarick, Chad Martin, Helena Johnston, Joe Clemente, and Hilary Burns (collectively "Plaintiffs") bring this Class Action Complaint ("Complaint") against Drug and Alcohol Treatment Services, Inc. ("DATS" or "Defendant") as an individual and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

SUMMARY OF ACTION

1. Plaintiffs and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted with sensitive Personally Identifiable Information ("PII")[1] and Protected Health Information ("PHI," and collectively with "PII," "Private Information") that was impacted in a data breach that Defendant publicly disclosed on May 2, 2025 (the "Data Breach" or the "Breach").

2. Plaintiffs' claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. Defendant is a private, non-profit agency that provides comprehensive outpatient treatment services to victims of substance abuse disorders.

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiffs and Class

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. On or around October 6, 2024, Defendant became aware of suspicious activity on its IT Network.[2] In response, Defendant launched an investigation to determine the nature and scope of the incident.[3]

6. Defendant's investigation determined that between October 5, 2024, and October 6, 2024, an unauthorized third-party accessed its IT Network and certain information contained within its IT Network.[4]

7. Upon information and belief, the following types of Private Information may have been compromised as a result of the Data Breach: name, date of birth, diagnosis information, individual insurance or subscriber number, member claims information, other health insurance information, patient account number, Social Security number, medical histories, financial information, health information, medical services information, and treatment information.[5]

8. On May 2, 2025, Defendant issued a public notice of the Data Breach and began sending letters to individuals impacted.[6] So, Defendant waited nearly seven months to notify the public that they were at risk.

9. As a result of this delayed response, Plaintiffs and Class Members had no idea for nearly seven months that their Private Information had been compromised, and that they were, and

---

[2] By way of example, Shawn Toolan's Notice Letter is attached as ***Exhibit 1.***

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

10. Defendant failed to take precautions designed to keep individuals' Private Information secure.

11. Defendant owed Plaintiffs and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

12. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiffs and Class Members have suffered irreparable harm. Plaintiffs and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

13. Defendant failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiffs and Class Members, causing the exposure of Plaintiffs' and Class Members' Private Information.

14. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

15. Upon information and belief, Defendant failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had Defendant properly monitored its networks, it would have discovered the Breach sooner.

16. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct as the Private Information that Defendant collected and maintained is now in the hands of data thieves and other unauthorized third parties.

17. There has been no assurance offered by Defendant that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

18. As a result of Defendant's inadequate digital security and notice process, Plaintiffs' and Class Members' Private Information was exposed to criminals. Plaintiffs and Class Members have suffered and will continue to suffer injuries, including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and, theft of personal and financial information.

19. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiffs and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

20. Plaintiffs bring this action against Defendant for: negligence; negligence *per se*, breach of contract, breach of implied contract; breach of confidence; and unjust enrichment, breach of fiduciary duty, and declaratory judgement.

21. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves, and all similarly situated persons, whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under 42 Pa.C.S. § 931.

23. This Court has personal jurisdiction over Defendant because Defendant is registered to do business and maintains its principal places of business in Lackawanna County, Pennsylvania.

24. Venue is proper pursuant to 42 Pa.C.S. § 931(c) because two Plaintiffs and Defendant are residents of Lackawanna County, Pennsylvania.

PARTIES

25. Plaintiff Leo Woytach is a resident and citizen of Scranton, Pennsylvania.

26. Plaintiff Shawn Toolan is a resident and citizen of Jessup, Pennsylvania.

27. Plaintiff James Davis is a resident of Forest City, Pennsylvania.

28. Plaintiff Bryce Allen is a resident of German, Pennsylvania.

29. Plaintiff Scott Stolarik is a resident of Peckville, Pennsylvania.

30. Plaintiff Chad Martin is a resident of Nescopeck, Pennsylvania.

31. Plaintiff Helena Johnston is a resident of Scranton, Pennsylvania.

32. Plaintiff Joe Clemente is a resident of Dunmore, Pennsylvania.

33. Plaintiff Hilary Burns is a resident of Scranton, Pennsylvania.

34. Defendant is a private, non-profit outpatient drug and alcohol treatment center based in Pennsylvania, with its principal place of business located at 441 Wyoming Avenue, Scranton, Pennsylvania, 18503.

FACTUAL ALLEGATIONS

Defendant's Business

35. Defendant is a private, non-profit agency that provides comprehensive outpatient treatment services to victims of substance abuse disorders.[7]

36. As a condition of receiving drug and alcohol treatment services, Defendant requires that its patients entrust it with highly sensitive personal and health information. In the ordinary course of receiving service from Defendant, Plaintiffs and Class Members were required to provide their Private Information to Defendant, including but not limited to the Private Information compromised in the Data Breach. Furthermore, Defendant stores and maintains the Private Information of thousands of its current and former patients.

37. Upon information and belief, Defendant made promises and representations to individuals, including Plaintiffs and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.[8]

38. Specifically, Defendant states in the first sentence of its Privacy Policy webpage: "[t]his privacy policy has been compiled to better serve those who are concerned with how their 'Personally identifiable information' (PII) is being used online." This statement indicates that Defendant is fully aware of the sensitivity and significance of PII to individuals.

---

[7] *About DATS*, DATS, https://www.datsrecovery.org/about-dats (last visited Sep. 12, 2025).

[8] *Privacy Policy*, DATS, https://www.datsrecovery.org/privacy-policy (last visited May 13, 2025).

39. Defendant further represents: "We do not sell, trade, or otherwise transfer Personally Identifiable Information."[9]

40. Upon information and belief, Defendant has made additional misleading representations to patients receiving services, beyond the statements published on its website. However, Defendant failed to uphold its promises to adequately safeguard Plaintiff's and Class Members' sensitive Private Information.

41. Plaintiffs and the Class Members relied on Defendant's promises to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

42. Thus, due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, Defendant, upon information and belief, promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

43. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

---

[9] *Id.*

The Data Breach

44. On or around October 6, 2024, Defendant became aware of suspicious activity on its IT Network. In response, Defendant launched an investigation to determine the nature and scope of the incident.[10]

45. Defendant's investigation determined that between October 5, 2024, and October 6, 2024, an unauthorized third-party accessed its IT Network and certain information contained within its IT Network.[11]

46. While cybercriminals maintained access to Defendants' systems for two consecutive days—October 5 and 6, 2024—Defendants failed to detect or stop the ongoing intrusion. This failure highlights Defendants' lack of adequate cybersecurity safeguards, as well as their noncompliance with industry standards and insufficient sensitivity to the risks associated with storing consumers' Private Information.

47. Upon information and belief, the following types of Private Information may have been compromised as a result of the Data Breach: name, date of birth, diagnosis information, individual insurance or subscriber number, member claims information, other health insurance information, patient account number, financial information, Social Security number, and medical services and treatment information of at least 22,000 individuals.

48. On May 2, 2025, roughly seven months after Defendant learned that the Class's Private Information was first accessed by cybercriminals, Defendant finally issued a public notice of the Data Breach and began sending letters to individuals impacted.[12]

---

[10] *Id.*

[11] *Id.*

[12] *Id.*

49. Omitted from the Notice are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

50. Thus, Defendant's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

51. In addition, the Notice offers no substantive steps to help victims like Plaintiffs and Class Members to protect themselves other than providing one year of credit monitoring – an offer that is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiffs and Class Members now face as a result of the Data Breach.

52. Defendant failed to take precautions designed to keep individuals' Private Information secure.

53. Defendant failed in upholding its duties to Plaintiff and Class Members when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Private Information. As such, Defendant's negligence has caused widespread injury and monetary damages to Plaintiff and Class Members.

54. While Defendant sought to minimize the damage caused by the Data Breach, Defendant cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiffs and Class Members.

55. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

Data Breaches Are Preventable

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

57. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing Private Information.

58. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

59. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

60. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[13]

[13] FBI, HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

61. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[14]

62. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-Facing Assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

[14] *Id.* at 3-4.

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[15]

63. Given that Defendant was storing Private Information, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

64. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of more than 22,000 individuals, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores Individuals' Private Information

65. Defendant acquires, collects, and stores individuals' Private Information.

66. Defendant requires that patients and other personnel entrust it with highly sensitive personal information.

67. By obtaining, collecting, and using Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

68. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

69. Upon information and belief, in the course of collecting Private Information from individuals, including Plaintiffs, Defendant promised to provide confidentiality and adequate

[15] *See Human-Operated Ransomware Attacks: A Preventable Disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

70. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew, or Should Have Known, of the Risk Because Healthcare Entities in Possession of Private Information Are Particularly Susceptible to Cyber Attacks

71. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the breach.

72. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

73. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[16]

74. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

[16] *See Victim Help Center,* ITRC, https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last visited Sep. 12, 2025).

75. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, cybercriminals often target small businesses, "because small businesses often lack the small business cybersecurity resources and response plans to fight back."[17]

76. Additionally, as companies became more dependent on computer systems to run their business,[18] e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[19]

77. Defendant knew and understood unprotected or exposed Private Information in the custody of insurance companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

78. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

---

[17] *Why Small Businesses are the New Cyber Targets*, Cyber Security Group, https://www.cybersecuritycloud.com/blog/cybersecurity-for-small-businesses#:~:text=Ransomware%20and%20phishing%20attacks%20are,over%20credentials%20or%20downloading%20malware (last viewed September 26, 2025).

[18] Danny Brando et al., *Implications of Cyber Risk for Financial Stability*, Bd. of Governors of the Fed. Rsrv. Sys. (May 12, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.

[19] Suleyman Ozarslan, *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, PICUS (Mar. 24, 2022), https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.

79. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

80. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

81. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

82. As a healthcare entity in custody of the Private Information, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

83. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[20]

[20] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-

84. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[21] In 2022, the largest growth in compromises occurred in the healthcare sector.[22]

85. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[23]

86. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[24]

87. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they

---

management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on May 13, 2025).

[21] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC_2018-EOY-BREACH-REPORT-KEY-FINDINGS.pdf (last visited on May 13, 2025).

[22] Identity Theft Resource Center, *2022 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on May 13, 2025).

[23] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on May 13, 2025).

[24] *Id.*

sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[25]

88. As a healthcare provider, Defendant knew, or should have known, the importance of safeguarding its patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on Defendant's patients as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

Value of Private Information

89. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[26] 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."[27]

---

[25] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on May 13, 2025).

[26] 17 C.F.R. § 248.201 (2013).

[27] *Id.*

90. The PII of individuals 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.[28]

91. For example, Personal Information can be sold at a price ranging from $40 to $200.[29] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[30]

92. Moreover, Social Security numbers, which were compromised for some Class Members in the Data Breach, are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

93. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [31] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[32]

---

[28] Anita George, *Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs,* DIGITALTRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[29] Ben Luthi, *Here's What Your Data Sells 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/.

[30] *For Sale In the Dark*, IN THE DARK, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Sep. 12, 2025).

[31] *See Avoid Identity Theft: Protect Social Security Numbers,* SOC. SEC., https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases (last visited Sep. 12, 2025).

[32] *Id.*

94. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[33]

95. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[34] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[35]

96. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[33] SOCIAL SECURITY ADMINISTRATION, IDENTITY THEFT AND YOUR SOCIAL SECURITY NUMBER, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sep. 12, 2025).

[34] *See How to Protect Yourself from Social Security Number Identity Theft,* EQUIFAX, https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited Sep. 12, 2025).

[35] *See* Julia Kagan, *What Is an SSN? What to Know About Social Security Numbers*, INVESTOPEDIA (Sep. 2, 2024), https://www.investopedia.com/terms/s/ssn.asp.

97. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[36]

98. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiffs' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.")

99. Similarly, the California state government warns patients that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of

[36] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[37]

100. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[38]

101. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

102. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[39] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[40] In short, these sorts of data breaches are

---

[37] *See Your Social Security Number: Controlling the Key to Identity Theft*, ROB BONTA ATT'Y GEN., https://oag.ca.gov/idtheft/facts/your-ssn (last visited Sep. 12, 2025).

[38] *Medical I.D. Theft*, EFraudPrevention, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited Nov. 6, 2023).

[39] Adil Hussain Seh et al., *Healthcare Data Breaches: Insights and Implications*, Nat'l Libr. of Med. (May 13, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/.

[40] Steve Alder, *December 2019 Healthcare Data Breach Report*, THE HIPPAA J. (Jan. 21, 2020), https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.

increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[41]

103. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[42]

104. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[43]

105. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[44] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[45]

---

[41] Juan Perez, *Cybersecurity Snapshot: Security Lags Cloud and AI Adoption, Tenable Report Finds, as CISA Lays Out Vision for CVE Program's Future*, TENABLE (Sep. 12, 2025), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/.

[42] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, NAKED SEC. (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

[43] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

[44] *See* Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[45] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/ (last accessed July 24, 2023).

106. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[46]

107. 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, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, PHI, dates of birth, and names.

108. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

109. The fraudulent activity resulting from the Data Breach may not come to light for years. 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.[47]

---

[46] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[47] U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 29 (2007), https://www.gao.gov/assets/gao-07-737.pdf.

110. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendant Fails to Comply with FTC Guidelines

111. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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.

112. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[48]

113. 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.[49]

114. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require

---

[48] FEDERAL TRADE COMMISSION, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[49] *Id.*

complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

115. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

117. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

118. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected

by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[50]

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

120. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information of individuals' or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

121. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of individuals, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendant Fails to Comply with HIPAA Guidelines

122. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security 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.

[50] FTC Commissioner Pamela Jones Harbour Remarks Before FTC Exploring Privacy Roundtable (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

123. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[51] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

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

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

126. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

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

128. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

129. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

130. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

[51] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

131. HIPAA's 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.

132. HIPAA also requires Defendant to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

133. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

134. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[52]

135. HIPAA requires a covered entity to have and apply appropriate sanctions against patients of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

136. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

137. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e- and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[53] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good

---

[52] *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Sep. 12, 2025) (emphasis added).

[53] *Security Rule Guidance Material*, U.S. DEP'T OF HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Sep. 12, 2025).

business practices with respect to standards for securing e-." US Department of Health & Human Services, Guidance on Risk Analysis.[54]

138. Based upon Defendant's Notice to Plaintiffs and Class Members, Defendant reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

139. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

140. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

141. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

142. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

---

[54] *Guidance on Risk Analysis,* U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Sep. 12, 2025).

143. In addition, Defendant's Data Breach could have been prevented if Defendant had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

144. Defendant's security failures also 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 Defendant creates, receives, maintains, and transmits 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 Defendant's workforce, 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.*

145. Because Defendant has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Defendant's approach to information security is adequate and appropriate going forward. Defendant still maintains the PHI and other highly sensitive PII of its current and former patients, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

Defendant Fails to Comply with Industry Standards

146. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

147. 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.[55]

148. 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.

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

[55] *The 18 CIS Critical Security Controls*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/controls/cis-controls-list (last visited on May 13, 2025).

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; (b) 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 (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[56]

150. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry-best practices, including a failure to implement multi-factor authentication.

151. Other best cybersecurity practices that are standard for healthcare entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

---

[56] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited May 13, 2025).

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its patients Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

156. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

157. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

158. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of

future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant.

Common Injuries & Damages

159. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) 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.

Data Breaches Increase Victims' Risk of Identity Theft

160. As Plaintiffs have already experienced, the unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers. As the Bureau of Justice Statistics reports, identity theft causes its victims out-of-pocket monetary losses and costs the nation's economy billions of dollars every year.[57]

[57] *See Victims of Identity Theft, 2012,* U.S. DEPT. OF JUSTICE, BUREAU OF JUSTICE STATISTICS (Dec. 2013), https://bjs.ojp.gov/content/pub/pdf/vit12.pdf.

161. The Private Information exposed in the Data Breach is highly coveted and valuable on underground or black markets. A cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web," exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Private Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; and (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

162. Consumers are injured every time their data is stolen and placed on the Dark Web, even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

163. Exposure of this information to the wrong people can have serious consequences. Identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2018-2020 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans and mortgages.[58] For some victims, this could

[58] *See 2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last visited Aug. 2 2024).

mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

164. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

165. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

166. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

167. Indeed, the fear that Plaintiffs data was exposed to nefarious actors has come to fruition—the Interlock ransomware group claimed responsibility for infiltrating Defendant's systems and stealing an alleged 150 GB of Plaintiffs' Private Information.[59]

168. Interlock held that Private Information for ransom—which was not paid—so Interlock published the Private Information on its website.[60]

---

[59] Steve Adler, *Drug and Alcohol Treatment Services Facing Multiple Class Action Data Breach Lawsuits*, THE HIPPA J. (June 9, 2025), https://www.hipaajournal.com/drug-and-alcohol-treatment-services-class-action-data-breach-litigation/.

[60] *Id.*

169. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[61]

170. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective patients."[62]

171. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a patient's identity after the initial account setup[.]"[63] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"[64]

---

[61] *See* N.C. GEN. STAT. § 132-1.10(1) (2025).

[62] *See* Husayn Kassai, *BankThink Banks Need to Stop Relying on Social Security Numbers*, AM. BANKER (Nov. 12, 2018, at 10:07 EST), https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers.

[63] *See* Ann Carrns, *Just 5 Banks Prohibit Use of Social Security Numbers*, THE N.Y. TIMES (Mar. 20, 2013, at 10:59 EST), https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/.

[64] *See* Nikkita Walker, What Can Someone Do with Your Social Security Number?. credit.com (Oct. 19, 2023), https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

172. The unauthorized disclosure of Social Security numbers can be particularly damaging because Social Security numbers cannot easily be replaced. To obtain a new number, a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until damage has been done. Furthermore, as the Social Security Administration warns:

> [A] new number probably won't solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service 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 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.
>
> If you receive a new Social Security number, you shouldn't use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.[65]

173. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[66]

---

[65] *See Identity Theft and Your Social Security Number* (July 2021), Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 20, 2025).

[66] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground*

174. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

175. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

176. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiffs and the other Class Members.

177. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

178. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Stolen From Texas Life Insurance Firm, KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

179. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the 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.[67]

Loss of Time to Mitigate Risk of Identity Theft & Fraud

180. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

181. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiffs and Class Members to take certain measures to protect themselves.

182. Defendant's extensive suggestion of steps that Plaintiffs and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant time that Plaintiffs and Class Members must undertake in response to the Data Breach. Plaintiffs' and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiffs and

---

[67] *Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown,* U.S Gov't Acct. Off. Rep. to Cong. Requesters (June 2007), http://www.gao.gov/new.items/d07737.pdf.

Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendant's Notice Letter.

183. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, signing up for the credit monitoring services offered by Defendant, and monitoring their financial accounts for any unusual activity, which may take years to detect. Accordingly, the Data Breach has caused Plaintiffs and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

184. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[68]

185. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[69]

---

[68] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007), https://www.gao.gov/new.items/d07737.pdf.

[69] *See What To Do Right Away,* FED. TRADE COMM'N, https://www.identitytheft.gov/Steps (last visited Sep. 12, 2025).

186. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[70]

Diminution of Value of Private Information

187. PII and PHI are valuable property rights. Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

188. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[71]

189. An active and robust legitimate marketplace for PII also exists. It has been estimated that the data brokering industry is worth roughly $200 billion.[72]

---

[70] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 2 (2007), https://www.gao.gov/new.items/d07737.pdf.

[71] *See, e.g.,* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[72] https://usa.kaspersky.com/resource-center/preemptive-safety/how-to-stop-data-brokers-from-selling-your-personal-information (last visited September 26, 2025).

190. In fact, the data marketplace is so sophisticated that patients can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[73]

191. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[74]

192. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[75]

193. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

194. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the

---

[73] *The Personal Data Revolution*, DATACOUP, https://datacoup.com/ (last visited Sep. 12, 2025); David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, L.A. TIMES (Nov. 5, 2019, at 5:00 PT), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[74] https://www.thepennyhoarder.com/make-money/nielsen-panel/ (last visited September 26, 2025).

[75] *Medical I.D. Theft*, EFRAUDPREVENTION https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited Nov. 6, 2023).

foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

195. The fraudulent activity resulting from the Data Breach may not come to light for years.

196. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

197. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[76] After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding $10,000;
- 40-percent were unable to pay bills;
- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and
- 51-percent suffered from panic of anxiety attacks.[77]

198. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to more than 22,000 individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

---

[76] *2023 Consumer Impact Report*, ITRC (Aug. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf.

[77] *Id.* at 21–25.

199. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

200. Given the type of targeted attack in this case, sophisticated criminal activity, the type of Private Information involved, and Plaintiffs' Private Information already being disseminated on the dark web, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

201. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

202. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

203. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

204. Furthermore, Defendant's poor data security practices deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for

medical products and/or services, Plaintiffs and other reasonable individuals understood and expected that they were, in part, paying for the services and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

205. As the result of the Data Breach, Plaintiffs and Class Members are likely to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Private Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

d. lowered credit scores resulting from credit inquiries following fraudulent activities;

e. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

f. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being in the possession of one or many unauthorized third parties.

Plaintiffs' Experiences

Plaintiff Leo Woytach's Experience

206. Plaintiff Leo Woytach ("Plaintiff Woytach") was a client of Defendant. As a condition to receiving services, he was required to and did provide his Private Information to Defendant which was then entered into Defendant's systems and maintained on its network.

207. Plaintiff Woytach greatly values his privacy and Private Information, especially when submitting information related to drug treatment and health care. Prior to the Data Breach, Plaintiff took reasonable steps to maintain the confidentiality of his Private Information, e.g., Plaintiff Woytach stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents; moreover, he diligently selects unique usernames and passwords on his various accounts; and he has not knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

208. Plaintiff Woytach received a letter dated May 2, 2025 from Defendant concerning the Data Breach. The letter states that unauthorized actors gained access to files on Defendant's network, which included Plaintiff's Private Information.

209. In addition, Plaintiff Woytach now receives many spam emails, which was not typical before the Data Breach. He cannot figure out any other explanation than that it is related to Defendant's Data Breach, which included his Private Information.

210. Since learning of the Data Breach, Plaintiff Woytach has heeded Defendant's advice and warnings and spent additional time in response to the Data Breach. One specific

example of time spent include that since the Data Breach, Plaintiff Woytach monitors his financial accounts and has signed up for LifeLock. Through LifeLock, he saw repeated fraudulent activity in the form of bank accounts attempting to be opened in his name and fraudulent transaction attempts, and he received Google notifications that his information was on the dark web.

211. Due to the Data Breach, Plaintiff has signed up for LifeLock credit monitoring services. This is more time than he spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes his time as a result of Defendant's negligence. Plaintiff Woytach plans on taking additional time-consuming necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing bank, credit and other accounts for unauthorized activity.

212. The Data Breach has caused Plaintiff Woytach to suffer anxiety and stress, which has been compounded by the fact that Defendant has not been forthright about the cause and full scope of the Private Information compromised in the Data Breach.

213. Plaintiff Woytach has lost confidence in his health care provider— Defendant — because of its failure to protect his medical records and medical information.

214. Plaintiff Woytach has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches and that the confidentiality of his medical records and information is maintained.

Plaintiff Shawn Toolan's Experience

215. Plaintiff Shawn Toolan ("Plaintiff Toolan") is a former patient of Defendant. On May 2, 2025, Defendant sent Plaintiff a notice letter informing him that his Private Information was compromised in the Data Breach.

216. Defendant was in possession of Plaintiff's Private Information before, during and after the Data Breach.

217. Plaintiff Toolan reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Toolan would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

218. Plaintiff Toolan was notified by Defendant that his private information was compromised in the Data Breach.

219. Plaintiff Toolan greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Toolan is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

220. Plaintiff Toolan stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

221. To the best of Plaintiff Toolan's knowledge, his PII has not been compromised in a prior data breach.

222. As a result of the Data Breach, Plaintiff Toolan has spent considerable time researching the Data Breach, reviewing his bank accounts, monitoring his credit report, changing his passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Toolan

spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

223. As a consequence of and following the Data Breach, Plaintiff Toolan has experienced a significant uptick in spam calls, text messages, and emails.

224. The Data Breach has caused Plaintiff Toolan to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in noticing him of the fact that his Social Security number in conjunction with his date of birth was acquired by criminals as a result of the Data Breach.

225. Plaintiff Toolan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Toolan will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

227. As a direct and traceable result of the Data Breach, Plaintiff Toolan suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his Private Information; (d) emotional distress because identity thieves now possess his first and last name paired with her Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and

identity theft now that his Private Information has been stolen and likely published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff; and (g) other economic and non-economic harm.

Plaintiff James Davis's Experience

228. Plaintiff James Davis ("Plaintiff Davis") provided his Private Information to DATS in connection with utilizing DATS's services as a drug and alcohol treatment center. In requesting and maintaining Plaintiff Davis's Personal Information for its business purposes, DATS impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Davis's Personal Information. DATS did not take proper care of Plaintiff Davis's Personal Information, leading to its theft as a direct result of DATS's inadequate security measures and data protection protocols.

229. Plaintiff Davis received a letter indicating that his PII may have been exposed in the DATS data breach.

230. Once Personal Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Davis will need to maintain heightened measures for years, and possibly his entire life.

231. Plaintiff Davis experienced unauthorized charges on his credit cards and received multiple spam emails informing him that his PayPal account has paid for subscriptions that he did not authorize. Experian Notices informed him that there were unemployment investigations undertaken in his name that he did not authorize.

232. Plaintiff Davis also suffered actual injury from having Personal Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential personal information—a form of property that Plaintiff Davis entrusted to DATS, which was compromised as a result of the Data Breach and (b)

a violation of Plaintiff Davis's privacy rights as a result of unauthorized disclosure of Personal Information.

233. As a result of the Data Breach, Plaintiff Davis made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Davis has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

234. As a result of the Data Breach, Plaintiff Davis has suffered anxiety as a result of the release of his PII and PHI, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII and PHI for purposes of committing cyber and other crimes against him including, but not limited to, fraud and identity theft. Plaintiff Davis is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on his life.

235. Had Plaintiff Davis known that DATS does not adequately protect PII, Plaintiff Davis would not have used DATS's services and agreed to provide DATS with his PII.

236. As a result of DATS's failure to adequately safeguard Plaintiff Davis's information, Plaintiff has been injured. Plaintiff Davis also is at a continued risk of harm because Plaintiff Davis's information remains in DATS's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

Plaintiff Scott Stolarik's Experience

237. Plaintiff Scott Stolarik (Plaintiff Stolarik") was a client of Defendant. As a condition to receiving services, Plaintiff Stolarik was required to and Plaintiff Stolarik provided his Private Information to Defendant which was then entered into Defendant's systems and maintained on its network.

238. Plaintiff Stolarik greatly values his privacy and Private Information, especially when submitting information related to health care. Prior to the Data Breach, Plaintiff Stolarik took reasonable steps to maintain the confidentiality of his Private Information, e.g., he stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents; moreover, he diligently selects unique usernames and passwords on his various accounts; and he has not knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

239. Plaintiff Stolarik received a letter dated May 2, 2025 from Defendant concerning the Data Breach. The letter states that unauthorized actors gained access to files on Defendant's network, which included Plaintiff Stolarik's Private Information.

240. In addition, Plaintiff Stolarik receives *many* spam calls and texts, which was not typical before the Data Breach. He cannot figure out any other explanation than that it is related to Defendant's Data Breach which included his Private Information.

241. Since learning of the Data Breach, Plaintiff Stolarik has heeded Defendant's advice and warnings and spent additional time in response to the Data Breach. This is more time than he spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes his time as a result of Defendant's negligence.

242. Due to the Data Breach, Plaintiff Stolarik plans on taking additional time-consuming necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing bank, credit and other accounts for unauthorized activity.

243. Plaintiff Stolarik has been informed by his bank that his Social Security number was leaked onto the dark web.

244. The Data Breach has caused Plaintiff Stolarik to suffer anxiety, depression, and stress, which has been compounded by the fact that Defendant has not been forthright about the cause and full scope of the Private Information compromised in the Data Breach.

245. Plaintiff Stolarik has lost confidence in his health care provider— Defendant — because of its failure to protect his medical records and medical information.

246. Plaintiff Stolarik has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches and that the confidentiality of his medical records and information is maintained.

Plaintiff Bryce Allen's Experience

247. On or about May 2, 2025, Defendant sent Plaintiff Bryce Allen ("Plaintiff Allen") the Notice Letter, stating that his Private Information was exposed in the Data Breach between October 5 and October 6, 2025.

248. Following the Data Breach, Plaintiff Allen experienced a substantial uptick in the number and frequency of spam calls.

249. Plaintiff Allen made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach; reviewing financial account statements

for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services; and dealing with unwanted spam calls.

250. Since Plaintiff Allen received Defendant's Notice Letter, he has already spent several hours dealing with the Data Breach, which is valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

251. As a result of the Data Breach, Plaintiff Allen has suffered emotional distress due to the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Allen is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

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

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

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

Plaintiff Chad Martin's Experience

255. On or about May 2, 2025, Defendant sent Plaintiff Chad Martin ("Plaintiff Martin") the Notice Letter, stating that his Private Information was exposed in the Data Breach between October 5 and October 6, 2025.

256. Following the Data Breach, Plaintiff Martin experienced a substantial uptick in the number and frequency of spam calls. Additionally, Plaintiff Martin has experienced misuse of his Private Information. After the Data Breach occurred, in or around November 2024, a PayPal account was opened in Plaintiff Martin's name without authorization. Plaintiff Martin has likewise identified various fraudulent activities associated with his credit accounts because of the Data Breach, such as multiple unauthorized credit card and loan applications under Plaintiff Martin's name. As a result, Plaintiff Martin's credit score dropped from 698 to approximately 400.

257. Plaintiff Martin made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach; reviewing financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services; and dealing with unwanted spam calls.

258. Since Plaintiff Martin received Defendant's Notice Letter, he has already spent several hours dealing with the Data Breach, which is valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

259. As a result of the Data Breach, Plaintiff Martin has suffered emotional distress due to the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Martin is very concerned

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

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

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

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

Plaintiff Helena Johnston's Experience

263. On or about May 2, 2025, Defendant sent Plaintiff Helena Johnston ("Plaintiff Johnston") the Notice Letter, stating that her Private Information was exposed in the Data Breach between October 5 and October 6, 2025.

264. Following the Data Breach, Plaintiff Johnston experienced a substantial uptick in the number and frequency of spam calls. Plaintiff Johnston has also experienced two instances of fraud since the data breach: first, she received a pending charge on a T-Mobile bill that she disputed with Credit Karma a couple of months after the breach, and second, she has received at least two hospital bills from places she has not visited.

265. Plaintiff Johnston made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach; reviewing financial account

statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services; and dealing with unwanted spam calls and instances of fraud.

266. Since Plaintiff Johnston received Defendant's Notice Letter, she has already spent several hours dealing with the Data Breach, which is valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

267. As a result of the Data Breach, Plaintiff Johnston has suffered emotional distress due to the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Johnston is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

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

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

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

Plaintiff Joe Clemente's Experience

271. On or about May 2, 2025, Defendant sent Plaintiff Joe Clemente ("Plaintiff Clemente") the Notice Letter, stating that his Private Information was exposed in the Data Breach between October 5 and October 6, 2025.

272. Following the Data Breach, Plaintiff Clemente experienced fraudulent charges on his bank account. He spent time going in person to his bank and ultimately decided to close his account and change banks in order to prevent the continued unauthorized fraudulent charges.

273. Plaintiff Clemente made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach; reviewing financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services; and dealing with unwanted spam calls. Plaintiff Clemente reported the breach to all three credit bureaus via Credit Karma and froze his major credit cards.

274. Since Plaintiff Clemente received Defendant's Notice Letter, he has already spent several hours dealing with the Data Breach, which is valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

275. As a result of the Data Breach, Plaintiff Clemente has suffered emotional distress due to the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Clemente is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

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

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

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

Plaintiff Hilary Burns's Experience

279. On or about May 2, 2025, Defendant sent Plaintiff Hilary Burns ("Plaintiff Burns") the Notice Letter, stating that her Private Information was exposed in the Data Breach between October 5 and October 6, 2025.

280. Following the Data Breach, Plaintiff Burns experienced fraud in the form of receiving spam inquiries and/or bills from healthcare providers that were not places she had ever visited. She also experienced several unauthorized login attempts to her accounts.

281. Plaintiff Burns made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach; reviewing financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services; and dealing with unwanted spam calls. Plaintiff Burns also checked all three of her credit bureaus to ensure there had not been unauthorized charges or inquiries, and continues to monitor same to this day.

282. Since Plaintiff Burns received Defendant's Notice Letter, she has already spent several hours dealing with the Data Breach, which is valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

283. As a result of the Data Breach, Plaintiff Burns has suffered emotional distress due to the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Burns is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

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

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

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

CLASS ALLEGATIONS

287. Plaintiffs bring this class action pursuant 231 Pa.C.S. Ch. 1700, Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States who were impacted by the Data Breach publicly announced by Defendant in May 2025, including all who were sent notice of the Data Breach (the "Class").

288. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family patients.

289. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

290. Numerosity: The Class is so numerous that joinder of all individuals impacted by the Data Breach is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

291. Commonality: Common questions of law and fact exist as to all Class Members and predominate over any questions affecting solely individuals of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class Members, including the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

292. Typicality: Plaintiffs' claims are typical of those of the other individuals of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffers from the same violations of the law as each other individual of the Class.

293. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the

Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

294. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

295. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

296. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure

to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

299. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

300. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

301. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify Plaintiffs and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard individuals' Private Information; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

302. Plaintiffs reallege and incorporate by reference all of the above paragraphs, as if fully set forth herein.

303. Defendant requires individuals', including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

304. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to individuals, which solicitations and services affect commerce.

305. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

306. Defendant failed to inform Plaintiffs and Class Members that its systems were inadequate to safeguard sensitive Private Information and that transferring Private Information could lead to cybercriminals gaining access to sensitive Private Information.

307. 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 the Private Information were wrongfully disclosed.

308. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

310. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

311. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiffs or Class Members of the Data Breach until July 18, 2024 despite, upon information and belief, Defendant knowing shortly after February 26, 2024 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiffs and the Class.

312. 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 its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

313. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of receiving services from Defendant.

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

315. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has 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.

316. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

317. Defendant also had a duty to exercise appropriate clearinghouse practices to remove individuals' Private Information it was no longer required to retain pursuant to regulations.

318. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

319. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were 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.

320. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect 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. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

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

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

f. Failing to remove individuals' Private Information it was no longer required to retain pursuant to regulations; and,

g. 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.

321. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

322. Plaintiffs and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

323. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

324. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

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

326. 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.

327. 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 cyberattacks and data breaches in the healthcare industry.

328. Defendant has 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.

329. 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 the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

330. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

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

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

333. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has 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.

334. 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.

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

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

337. 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) invasion of privacy; (ii) theft of their Private Information; (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private Information being disseminated on the dark web, according to Identity Defense Complete; (ix) nominal damages; and (x) 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.

338. 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.

339. Additionally, as a direct and proximate result of Defendant's negligence, 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 its continued possession.

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

341. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

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

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)

343. Plaintiffs reallege and incorporate by reference all of the above paragraphs, as if fully set forth herein.

344. Pursuant to Section 5 of the FTCA, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

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

346. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "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.

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

348. Specifically, Defendant breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper

segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

349. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendant's duty in this regard.

350. Defendant also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

351. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendant's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

352. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and Defendant's failure to comply with both constitutes negligence *per se*.

353. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Defendant's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

354. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized

access of their Private Information, including but not limited to damages from the actual misuse of their Private Information and the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

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

356. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
Breach of Contract
(On Behalf of Plaintiffs and the Nationwide Class)

357. Plaintiffs reallege and incorporate by reference all of the above paragraphs, as if fully set forth herein.

358. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to Defendant in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

359. Defendant's Privacy Policy memorialized the rights and obligations of Defendant and its patients. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

360. In the Privacy Policy, Defendant commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

361. Plaintiffs and Class Members fully performed their obligations under their contracts with Defendant.

362. However, Defendant did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore Defendant breached its contracts with Plaintiffs and Class Members.

363. Defendant allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, Defendant breached the Privacy Policy with Plaintiffs and Class Members.

364. Defendant's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in Defendant providing services to Plaintiffs and Class Members that were of a diminished value.

365. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

366. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

367. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

368. Plaintiffs reallege and incorporate by reference all of the above paragraphs, as if fully set forth herein.

369. Plaintiffs plead this claim in the alternative to their other contract-based claims.

370. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of receiving healthcare services at Defendant.

371. Plaintiffs and the Class entrusted their Private Information to Defendant. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

372. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

373. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

374. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

375. In accepting the Private Information of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

376. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

377. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

378. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

379. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

380. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

381. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

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

383. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

384. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

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

386. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Nationwide Class)

387. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

388. In light of the special relationship between Defendant and its patients, whereby Defendant became a guardian of Plaintiffs' and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI) Defendant was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members. This benefit included (1) the safeguarding of Plaintiffs' and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where Defendant's patients' Private Information was and is stored.

389. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of its patients' relationship, in particular to keep the Private Information secure.

390. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently investigate the Data Breach to determine the number of Class Members affected and notify them within a reasonable and practicable period of time.

391. Defendant breached its fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

392. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

393. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

394. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

395. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; 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).

396. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 CFR 164.306(a)(2).

397. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

398. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

399. Defendant breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

400. 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 the harms and injuries

alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class)

401. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above as though fully set forth herein.

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

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

404. Plaintiffs and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

405. Plaintiffs and the Class also entrusted Defendant with their Private Information with the explicit and implicit understanding that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

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

407. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, 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.

408. As a direct and proximate cause of Defendant's actions and omissions, Plaintiffs and the Class have suffered damages.

409. But for Defendant's disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their 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.

410. The injury and harm Plaintiffs and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private Information. Defendant knew or should have known that its methods of accepting and securing Plaintiffs' and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and Class Members' Private Information.

411. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Class, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with

effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to 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 of individuals; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

412. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Class Members 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.

COUNT VII
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

413. Plaintiffs reallege and incorporate by reference all of the above paragraphs, as if fully set forth herein.

414. Plaintiffs bring this claim in the alternative to the breach of implied contract claim above.

415. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for healthcare services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members

should have received from Defendant the healthcare services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

416. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving healthcare services at Defendant. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

417. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

418. Thus, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

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

420. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

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

422. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

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

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

425. Plaintiffs and Class Members have no adequate remedy at law.

426. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of their Private Information consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiffs'

Private Information being disseminated on the dark web, according to Identity Defense Complete; (ix) statutory damages; (x) nominal damages; and (xi) 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.

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

(b) An order awarding injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as necessary to protect the interests of Plaintiffs and Class Member, including but not limited to, and order;

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendant to protect, including through encryption, all data collected through the course of their businesses in accordance with all applicable regulations, industry standards, and state or local laws;

iii. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. Prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

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

vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. Requiring Defendant to conduct regular database scanning and securing checks;

xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xii. Requiring Defendant to routinely and continually conduct internal training and education, and, on an annual basis, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting Private Information;

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. For a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment;

(c) For an order declaring that Defendant conduct violates the laws referenced herein;

(d) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(e) For damages in amounts to be determined by the Court and/or jury;

(f) For an award of statutory damages or penalties to the extent available;

(g) For pre-judgment interest on all amounts awarded;

(h) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

(i) For an order of restitution and all other forms of monetary relief; and

(j) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

[SIGNATURE BLOCK ON FOLLOWING PAGE]

Dated: October 3, 2025

By: _____

Samantha E. Holbrook (PA ID# 311829)
Benjamin F. Johns (PA ID #201373)
SHUB JOHNS & HOLBROOK LLP
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
(610) 477-8380
sholbrook@shublawyers.com
bjohns@shublawyers.com

Kenneth J. Grunfeld (PA ID# 84121)
KOPELOWITZ OSTROW P.A.
65 Overhill Road
Bala Cynwyd, PA 19004
(954) 525-4100
grunfeld@kolawyers.com

Interim Co-Lead Counsel

IN THE COURT OF COMMON PLEAS
OF LACKAWANNA COUNTY, PENNSYLVANIA

LEO WOYTACH, JAMES DAVIS, SHAWN TOOLAN, BRYCE ALLEN, SCOTT STOLARIK, CHAD MARTIN, HELENA JOHNSTON, JOE CLEMENTE, and HILARY BURNS, individually and on behalf of all others similarly situated, Plaintiffs, vs. DRUG AND ALCOHOL TREATMENT SERVICES, INC., Defendant.	Case No. 2025-CV-03681 CONSOLIDATED CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

VERIFICATION

I, Joe Clemente, hereby verify that I am a plaintiff in the above-captioned matter and the allegations set forth in the complaint are true and correct, to the best of my knowledge, information and belief, subject to the 18 Pa.CS § 4904.

Dated: 10/02/2025

josephclemente (Oct 2, 2025 13:38:59 EDT)

Joe Clemente

IN THE COURT OF COMMON PLEAS
OF LACKAWANNA COUNTY, PENNSYLVANIA

LEO WOYTACH, JAMES DAVIS, SHAWN TOOLAN, BRYCE ALLEN, SCOTT STOLARIK, CHAD MARTIN, HELENA JOHNSTON, JOE CLEMENTE, and HILARY BURNS, individually and on behalf of all others similarly situated, Plaintiffs, vs. DRUG AND ALCOHOL TREATMENT SERVICES, INC., Defendant.	Case No. 2025-CV-03681 CONSOLIDATED CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

VERIFICATION

I, Hilary Burns, hereby verify that I am a plaintiff in the above-captioned matter and the allegations set forth in the complaint are true and correct, to the best of my knowledge, information and belief, subject to the 18 Pa.CS § 4904.

Dated: 10/02/2025

Hilary Burns (Oct 2, 2025 14:07:20 EDT)

Hilary Burns

EXHIBIT 1

May 2, 2025

("DATS") writes to notify you of an incident that may impact the privacy

offering you access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you on the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services

What You Can Do: In addition to enrolling in the complimentary credit monitoring service detailed below, we recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits forms for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly change your password, contact the financial institution or company if applicable, and take any additional steps needed to protect your account. Additionally, please report any suspicious incidents to local law enforcement and/or your Attorney General. Please review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.