SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF ERIE

SUSAN SZUCS, ANTHONY PARRIZZI, TERRENCE ERNEST GIDNEY, CHRISTINA CHURCH, JIMMIE HARDAWAY, JR., SHARON SIEGLE, PAUL PASCUCCI, JAMES MARCISZEWSKI, and SHANNON ALLGRIM, individually and on behalf of all others similarly situated, Plaintiffs, v. EXCELSIOR ORTHOPAEDICS, LLP, and BUFFALO SURGERY CENTER, LLP, Defendants.	Index No.: 812753/2024 **CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Susan Szucs, Anthony Parrizzi, Terrence Ernest Gidney, Christina Church, Jimmie Hardaway, Jr., Sharon Siegle, Paul Pascucci, James Marciszewski, and Shannon Allgrim (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), bring this action against Defendants Excelsior Orthopaedics, LLP ("Excelsior") and Buffalo Surgery Center, LLP ("BSC," and collectively with Excelsior, "Defendants") to obtain damages, restitution, and injunctive relief from Defendants. Plaintiffs make the following allegations upon information and belief (except as to Plaintiffs' own actions), the investigation of counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of Defendants' failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiffs' and Class Members' sensitive personal identifiable and health information, including sensitive medical imaging/X-rays, that they acquired from their patients and stored for business purposes. These failures to secure and monitor their

networks and the sensitive information in their care resulted in a data breach of images and information of the *highest sensitivity* belonging to Defendants' patients.

2. Excelsior owns and/or operates ten different medical office locations throughout the western New York area that offer orthopedic specialists, an ambulatory surgery center, and other medical facilities. Excelsior works with seventeen school districts and has served over 400,000 patients since 2001. Excelsior is affiliated with BSC, a multispecialty ambulatory surgery center who provides orthopedics, total joint replacement, and endoscopy services to western New Yorkers and people in the surrounding area.

3. In the course of serving their patients and other affiliated persons and employing employees, Defendants collect a significant amount of data, including patient and employee personally identifiable information, legal name, demographic data, protected health information, sensitive medical imaging, and financial information.

4. On or about June 23, 2024, Excelsior became aware of a data security incident resulting in unauthorized access to certain personal and/or protected health information maintained in its systems (the "Data Breach").[1]

5. The information compromised in the Data Breach included the sensitive private information of current and former patients and employees of, and other persons affiliated with, Defendants and their related entities. Although the exact information disclosed may vary slightly based on the individual, the compromised private information included, but is not limited to: full name, address, date of birth, Social Security number, driver's license number, non-driver identification card number, biometric information, medical record number, diagnosis, diagnosis

[1] *Notice of Data Security Incident,* Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8561b966-2671-45c6-98eb-d7acff5e31b3.html (last visited June 3, 2025).

code, treatment location, procedure type, provider name, treatment cost, medical date of service, health insurance information, subscriber member number and patient account number, and medical imaging, including sensitive X-ray images of patients' bodies ("Private Information").

6. Despite learning of the Data Breach on or about June 23, 2024, Excelsior did not begin sending notices of the Data Breach until August 2024. Excelsior mailed a second wave of notices months later, in December 2024, to additional individuals identified as being affected by the Data Breach. BSC posted a notice of the Data Breach on its website on January 3, 2025.

7. Despite having the financial wherewithal and personnel necessary to prevent the Data Breach, Defendants failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they maintained for Plaintiffs and Class Members. The Data Breach was a direct and proximate result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals' Private Information with which they were entrusted for either treatment or employment, or both.

8. Plaintiffs' and Class Members' identities are now at risk because of Defendants' wrongful conduct, since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

9. Plaintiffs and Class Members have suffered injuries as a result of Defendants' conduct. These injuries include: (i) theft of their Private Information; (ii) lost or diminished value of Private Information; (iii) lost time (that Plaintiffs and Class Members could have dedicated to employment and recreation) associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; (viii) heightened and imminent risk of fraud, identity theft, and blackmail; and

(ix) the continued and certainly increased risk to their Private Information, which remains unencrypted and available for unauthorized third parties to access and abuse, and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information still in their possession.

10. Through this Complaint, Plaintiffs seek to remedy these harms individually and on behalf of the Class. Accordingly, Plaintiffs bring this action against Defendants seeking redress for their unlawful conduct, and asserting claims for (i) negligence, (ii) negligence per se, (iii) breach of contract, (iv) breach of implied contract, (v) breach of fiduciary duty, (vi) unjust enrichment, (vii) breach of confidence, and (viii) violations of New York General Business Law § 349.

11. Plaintiffs seek all available remedies, including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendants' data security systems, future annual audits (as well as long-term and adequate credit monitoring services funded by Defendants), and declaratory relief.

PARTIES

12. Plaintiff Susan Szucs is a resident and citizen of the State of New York.

13. Plaintiff Anthony Parrizzi is a resident and citizen of the State of New York.

14. Plaintiff Terrence Ernest Gidney is a resident and citizen of the State of Florida.

15. Plaintiff Christina Church is a resident and citizen of the State of New York.

16. Plaintiff Jimmie Hardaway, Jr. is a resident and citizen of the State of New York.

17. Plaintiff Sharon Siegle is a resident and citizen of the State of New York.

18. Plaintiff Paul Pascucci is a resident and citizen of the State of New York.

19. Plaintiff James Marciszewski is a resident and citizen of the State of New York.

20. Plaintiff Shannon Allgrim is a resident and citizen of the State of New York.

21. Defendant Excelsior Orthopaedics, LLP is a New York domestic registered limited liability partnership that has its principal place of business at 3925 Sheridan Drive, Amherst, New York 14226.

22. Defendant Buffalo Surgery Center, LLC is a limited liability company headquartered in Amherst, New York, with its principal place of business located at 3921 Sheridan Drive, Amherst, New York 14266.

JURISDICTION AND VENUE

23. The Court has personal jurisdiction over Defendants because, personally or through their agents, Defendants operate, conduct, engage in, or carry on business or business ventures in this State. The Court has jurisdiction pursuant to CPLR § 301, because Defendants maintain their principal places of business in the state of New York and conduct substantial business in the state of New York.

24. Venue is proper in this Court pursuant to CPLR § 503(a) because Defendants maintain their principal place of business in this County, conduct substantial business in this County, and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this County.

FACTUAL ALLEGATIONS

Defendants' Businesses

25. Excelsior touts itself as a pioneer in streamlined care. "From being the first to offer orthopedic urgent care to having in-house physical therapy, imaging, crutches and canes, sports performance, nutrition and outpatient surgery, your diagnosis, treatment and recovery can all take place right here."[2]

[2] EXCELSIOR ORTHOPAEDICS, http://www.excelsiorortho.com/ (last visited June 3, 2025).

26. Excelsior has over 100 Orthopaedic Specialists, 10 locations in the Western New York area, over 400,000 patient visits yearly, and provides 17 local school districts with expert athletic training.[3]

27. Excelsior claims its "mission is to transform the lives of … patients by restoring function and enhancing quality of life."[4]

28. Excelsior offers services such as general orthopedics, sports medicine, hand and upper extremity care, foot and ankle care, knee and leg care, hip care, and pain management.[5]

29. Defendant BSC is a multi-specialty ambulatory surgery center. It provides orthopedic services, total joint replacement, and gastroenterology & colorectal endoscopy services.[6] BSC is affiliated with and/or otherwise related to Excelsior, and Excelsior provides numerous administrative and IT-related services to BSC including data hosting.

30. In the ordinary course of receiving medical care services from Defendants, or alternatively being employed by Defendants, each patient and employee must provide (and Plaintiffs did provide) Defendants with sensitive, personal, and private information, such as all or some of the following:

- Name, address, phone number, email address;
- Date of birth;
- Social Security number;
- Marital status;
- Employer with contact information;

[3] *About Excelsior,* EXCELSIOR ORTHOPAEDICS, https://www.excelsiorortho.com/about/ (last visited June 3, 2025).
[4] *Id*.
[5] *Specialties of Care,* EXCELSIOR ORTHOPAEDICS, https://www.excelsiorortho.com/specialties/ (last visited June 3, 2025).
[6] *Services,* BUFFALO SURGERY CENTER, https://www.buffalosurgerycenter.com/services/ (last visited June 3, 2025).

- Primary and secondary insurance policyholders' name, address, date of birth, and Social Security number;
- Demographic information;
- Driver's license or state or federal identification;
- Information relating to the individual's medical condition and medical history;
- Insurance information and coverage; and
- Banking and/or credit card information.

31. Defendants also create and store medical records, including sensitive medical imaging/X-rays, records of treatments, diagnoses, and other Private Information for their patients.

32. Plaintiffs and Class Members transferred, and Defendants gathered, Private Information that was compromised in the Data Breach. This information was necessarily entrusted to Defendants' possession so that Plaintiffs could facilitate services from and/or employment with Defendants, but only with the agreement and understanding that the Private Information would be adequately safeguarded and/or destroyed within a reasonable time after the termination of the respective relationship.

33. By obtaining, collecting, receiving, and/or storing Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew, or should have known, that they were thereafter responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

34. Further, Excelsior has written privacy policies that it provides to patients. Upon information and belief, Excelsior's HIPAA notices and privacy policies are provided to every

patient both prior to receiving treatment and upon request.[7] Excelsior's Notice of Privacy Practices makes clear that it understands that its patients' Private Information is personal and must be protected by law.

35. In its Notice of Privacy Practices, Excelsior promises its patients that "uses and disclosures of your protected health information will be made only with your written authorization" and says that, as required by law, "[p]rior to disclosing your protected health information to outside health care providers or to obtain payment, Excelsior Orthopaedics ("Excelsior") will obtain your general consent, usually at your first visit to our facility."[8]

36. In part by virtue of Excelsior's Notice of Privacy Practices, and also due to the highly sensitive and personal nature of the information and images/X-rays Defendants acquire and store with respect to their patients, Defendants implicitly and/or explicitly promised to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of their patients' Private Information; inform patients of Defendants' 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 Defendants provide; and provide adequate notice to patients if their Private Information is disclosed without authorization.

37. Plaintiffs and the Class Members, as patients and/or employees of Defendants, relied on these promises and on these sophisticated business entities 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. Consumers and employees, in

[7] *Forms & Brochures*, EXCELSIOR ORTHOPAEDICS, https://www.excelsiorortho.com/patient-resources/forms-brochures/ (see link to "Notice of Privacy Practices") (last visited June 3, 2025).
[8] *Notice of Privacy Practices*, EXCELSIOR ORTHOPAEDICS, https://www.excelsiorortho.com/wp-content/uploads/2020/08/Excelsior_Forms_Notice-of-Privacy-Practices-02.18.2014.pdf (last visited June 3, 2025).

general, demand security to safeguard their Private Information, especially when their Social Security numbers and other sensitive Private Information are involved.

38. Defendants derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without that Private Information, Defendants could not have consummated their transactions with Plaintiffs and Class Members or carried on their business.

39. Defendants' actions and inactions directly resulted in the Data Breach and the compromise of Plaintiffs' and Class Members' Private Information.

The Data Breach

40. Excelsior learned of a cyberattack on its systems on or around June 23, 2024.[9]

41. In August of 2024, Excelsior sent an initial batch of letters entitled "Data Security Incident Involving Excelsior Orthopaedics, LLP" ("August Notice") to a small population of affected individuals informing them that its investigation determined that their Private Information was accessed.

42. The August Notice indicated that "[o]n June 23, 2024, Excelsior detected unusual activity on its network and discovered that it was the victim of a data security incident" and that the "[c]ompromised data may include information about employees of the Buffalo Surgery Center, a related entity."[10]

43. Per the August Notice, the Private Information that was compromised was an individual's full name, address, date of birth, Social Security number, driver's license number, non-driver identification card number, and biometric information.

44. On or about December 31, 2024, Excelsior sent a second batch of letters entitled Notice of Data Security Incident ("December Notice") to patients and employees.

[9] *Notice of Data Security Incident*, n.1, *supra*.
[10] *Id*.

45. The December Notice stated:[11]

> ***What Happened?***
>
> On June 23, 2024, Excelsior detected unusual activity on its network and discovered that it was the victim of a data security incident. Upon discovery of this incident, Excelsior immediately took steps to contain the intrusion and engage a specialized third-party cybersecurity firm to help secure the environment and conduct a comprehensive forensic investigation into the nature and scope of the incident. Initial findings from the forensic investigation indicated that the incident resulted in the compromise of data relating to current and former patients and employees of Excelsior and its related entities, including Buffalo Surgery Center and Northtowns Orthopaedics. In light of those findings, Excelsior engaged outside data mining experts to conduct a thorough analysis of the compromised data and identify affected individuals.
>
> In August 2024, with the data mining process ongoing, Excelsior mailed an initial wave of notices to a small population of affected individuals and reported the incident to the U.S. Department of Health and Human Services and the Office for Civil Rights. The bulk of data mining was completed in December 2024, which identified additional individuals for purposes of notification.
>
> ***What Information Was Involved?***
>
> Based on the data mining results, the following information related to you was impacted as a result of this incident: full name, Date of Birth, Medical Record Number, Diagnosis, Diagnosis Code, Treatment Location, Procedure Type, Provider Name, Treatment Cost, Medical Date of Service, Health Insurance Information, Subscriber Member Number and Patient Account Number. Note, impacted data varies based on the individual.
>
> […]
>
> ***What You Can Do***
>
> We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of

[11] *See Notice of Data Security Incident,* n.1, *supra* (then follow "1-7-25 Maine Final AG Notification" hyperlink).

> such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed Steps You Can Take to Help Protect Your Information, to learn more about how to protect against the possibility of information misuse.
>
> […]

46. BSC released information regarding the Data Breach on its website on January 3, 2025, where it said that is "is writing to provide information about a data security incident that affected one of our affiliates, Excelsior Orthopaedics, LLP []. Excelsior has worked closely with BSC for over 20 years and currently provides numerous administrative and IT-related services to BSC including data hosting. Excelsior's recent data security incident may have resulted in unauthorized access to sensitive personal information stored on Excelsior's computer network, including information pertaining to BSC patients."[12]

47. On information and belief, BSC was informed of the Data Breach by Excelsior and was involved in the identification of affected individuals and the notice process.

48. Based on Defendants' notices, it is clear that cybercriminals intentionally targeted Excelsior for the highly sensitive Private Information it stores on its computer network, attacked the insufficiently secured network, then exfiltrated highly sensitive Private Information. As a result, the Private Information of Plaintiffs and Class Members remains in the hands of those cybercriminals.

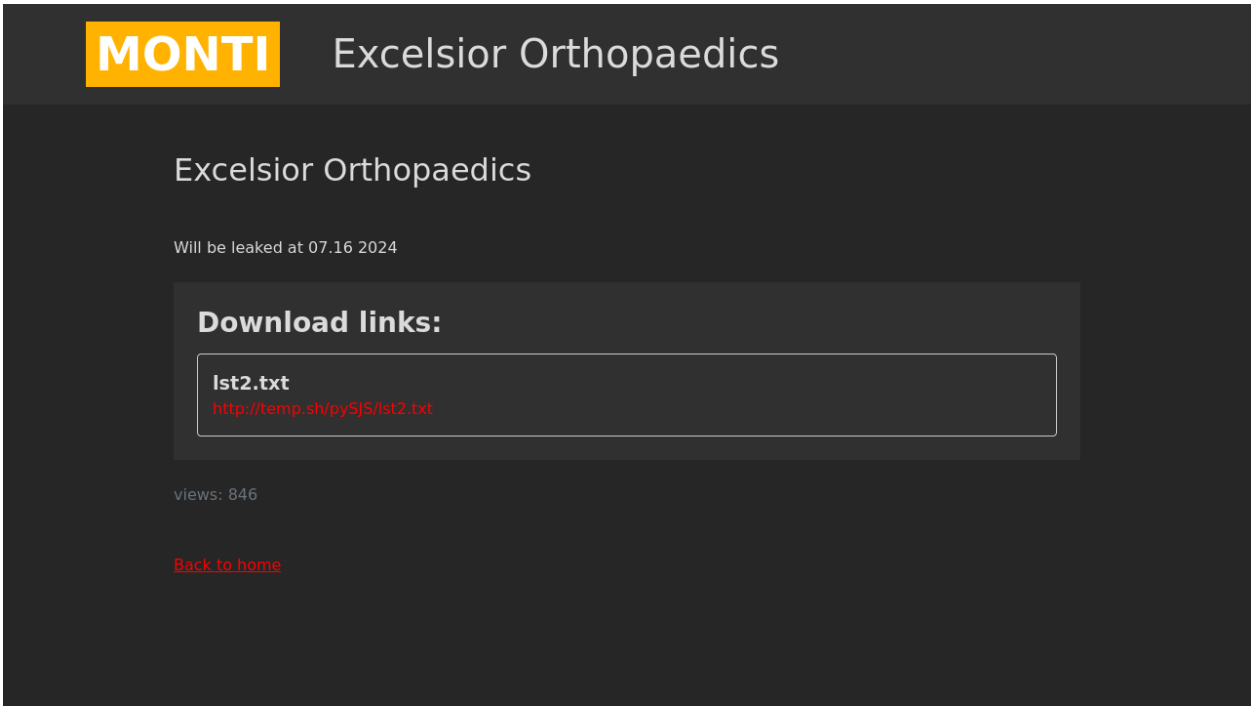
49. According to a notice Excelsior sent to the Maine Attorney General, the Private Information of approximately 357,000 individuals was implicated in the Data Breach.[13]

[12] *Notice of Data Incident*, BUFFALO SURGERY CENTER, January 3, 2025, https://www.buffalosurgerycenter.com/notice-of-data-incident/ (last visited June 3, 2025).
[13] *Notice of Data Security Incident,* n.1, *supra*.

50. The notorious MONTI ransomware gang claimed responsibility for the cyberattack. MONTI is one of the most active ransomware actors in existence, having breached hundreds of companies, including other healthcare entities, worldwide.[14] Defendants—self-proclaimed leaders in their industry—knew or should have known of the tactics that groups like MONTI employ.

51. With the Private Information secured and stolen by MONTI, the hackers then purportedly issued a ransom demand to Defendants. However, Defendants have provided no public information on the ransom demand or payment.

52. On information and belief, all stolen Private Information, including sensitive medical images/X-rays, was leaked onto the dark web on July 16, 2024—the ransom demand deadline.



[14] Monti Ransomware, AVERTIUM (Sept. 12, 2023), https://www.avertium.com/resources/threat-reports/monti-ransomware (last visited June 3, 2025).

53. Defendants' response to the Data Breach was woefully inadequate. Defendants took over two months to notify a "small population of affected individuals" that their data was breached and over six months to notify the remaining affected individuals. This means that for six months most Class Members had no knowledge that their Private Information was exposed.

54. Defendants failed to explain precisely how the Data Breach occurred, including how the unauthorized actors initially gained access to their systems and why Defendants failed to detect the intrusion(s) of these unauthorized actors. Further, Defendants failed to offer any sort of immediate compensation for the harm caused by their inadequate cybersecurity protections.

55. What is clear from the August and December Notices is that cybercriminals did, in fact, access, view, and exfiltrate for sale/financial leverage on the dark web Plaintiffs' and Class Members' Private Information, including highly sensitive images/X-rays, during the period in which the cybercriminals had unfettered access to Defendants' network, as that is the modus operandi of cybercriminals who commit such attacks.

56. Upon information and belief Defendants thus failed to: (1) ensure the proper monitoring and logging of the ingress and egress of network traffic; (2) ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions; (3) ensure the proper monitoring and logging of file access and modifications; (4) ensure the proper encryption of Plaintiffs' and Class Members' Private Information and monitor user behavior and activity to identify possible threats; (5) adequately train employees and cybersecurity partners on cybersecurity policies and then failed to enforce those policies; (6) maintain reasonable and adequate security practices over the systems storing Plaintiffs' and Class Members' Private Information; and (7) implement reasonable safeguards that would have prevented the Data Breach, despite being capable of doing so.

57. Plaintiffs and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

58. By requiring and accepting Plaintiffs' and Class Members' Private Information, Defendants agreed to and undertook legal duties to maintain the Private Information entrusted to them safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

59. Defendants' data security obligations were particularly important given the ubiquity of healthcare (and other) cyberattacks. As providers of healthcare, Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

The Data Breach Was a Foreseeable Risk of Which Defendants Were on Notice

60. Defendants had obligations created by HIPAA, industry standards, common law, and other promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

62. It is well known that Private Information, including Social Security numbers, is a valuable commodity and a frequent, intentional target of cybercriminals. Companies that collect this sensitive information are aware of the risk of cyberattacks.

63. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names,

taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, engaging in other medical identity theft, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

64. Individuals therefore place a high value not only on their Private Information, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

65. The likelihood of a company experiencing a data breach is apparent, as they are on the rise: during just the first half of 2024, there were a record 1,571 breaches reported during the six-month period, impacting an estimated 1.07 billion victims. According to the Identity Theft Resource Center, "[t]he numbers represent an increase in breaches of about 14% over the same period in 2023. That's notable considering that 2023 set a record for the number of data breaches reported in a single year with 3,203."[15]

66. Cybersecurity attacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and prepared for (and hopefully can ward off) a cybersecurity attack.

67. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[16]

[15] Bree Fowler, *About 1 Billion People Hit by Data Breaches in First Half of 2024*, CNET (July 18, 2024), https://www.cnet.com/tech/services-and-software/about-1-billion-people-hit-by-data-breaches-in-first-half-of-2024/.
[16] *How We Can Help* You, FBI.GOV, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware (last visited June 3, 2025).

68. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take the appropriate steps to protect the Private Information of Plaintiffs and the Class Members from being compromised.

69. Defendants' data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

70. According to an article in the HIPAA Journal, in 2024, [f]or the fourth consecutive year, more than 700 data breaches of 500 or more healthcare records were reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR)."[17]

71. The article goes on to say, "[d]ata breach severity has been increasing, with 2024 seeing some of the largest-ever data breaches" and that "[h]acking incidents accounted for the majority of healthcare data breaches last year."[18]

72. Although these breaches are common, "[b]ased on breach reporting at The HIPAA Journal, it is clear that many of the year's data breaches could have been prevented by implementing recognized security practices […]."[19]

73. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[20]

---

[17] Steve Alder, Editorial: *Lessons from 2024 Healthcare Data Breaches*, THE HIPAA JOURNAL (Jan. 24, 2025), https://www.hipaajournal.com/editorial-lessons-from-2024-healthcare-data-breaches/.
[18] *Id*.
[19] *Id*.
[20] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, THE HIPAA JOURNAL (Nov. 2, 2023), https://www.hipaajournal.com/why-do-criminals-target-medical-records/.

74. The HIPAA Journal article explains that patient records, like those stolen from Excelsior, are "often processed and packaged with other illegally obtained data to create full record sets . . . that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark websites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[21]

75. According to HIPAA statistics, between October 21, 2009, when OCR first started publishing summaries of data breach reports on its "Wall of Shame," and December 31, 2023, 5,887 large healthcare data breaches have been reported. Most of these data breaches are due to hacking:

> In 2023, OCR reported a 239% increase in hacking-related data breaches between January 1, 2018, and September 30, 2023, and a 278% increase in ransomware attacks over the same period. In 2019, hacking accounted for 49% of all reported breaches. In 2023, 79.7% of data breaches were due to hacking incidents. [22]

76. Per the HIPAA Journal, data breaches are increasing in scale as well as frequency. In 2021, 45.9 million healthcare records were breached; in 2022 there were 51.9 million records breached; and in 2023, there were 168 million records stolen.[23]

77. In the past few years, there have been many large healthcare-related data breaches with tens of millions of victims including HCA Healthcare (11,270,000 victims) in 2023, Perry Johnson & Associates (9,302,588 victims) in 2023, Change Healthcare (190,000,000 victims) in 2024, Anthem Inc. (78,800,000 victims) in 2024, and others.[24] As such, Defendants were aware of the risk of data breaches because such breaches have dominated the headlines recently.

---

[21] *Id.*
[22] Steve Alder, *Healthcare Data Breach Statistics*, THE HIPAA JOURNAL (May 26, 2025), https://www.hipaajournal.com/healthcare-data-breach-statistics/.
[23] *Id*.
[24] *Id*.

78. 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.[25]

79. In January of 2023, HHS created a presentation specifically for healthcare providers and IT departments, warning entities like Defendants of severe threats posed by Royal, BlackCat, and similar cybercriminal groups.[26] Within the healthcare industry, the risk of a cyberattack is well known and preventable with adequate security systems in place. The FBI has also specifically warned healthcare entities of the risks of data breaches, stating that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[27]

80. In fact, according to a 2024 report done by Proofpoint, 92% of healthcare organizations experienced cyberattacks in 2024.[28]

81. HHS data shows more than 39 million patients' information was exposed in the first half of 2023, in nearly 300 incidents, and that healthcare breaches have doubled between 2020 and 2023, according to records compiled from HHS data by Health IT Security.[29]

---

[25] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N. (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shutdown-clinics-hospitals.

[26] OFFICE OF INFORMATION SECURITY, *Royal & BlackCat Ransomware: The Threat to the Health Sector* (Jan. 12, 2023), https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf.

[27] Jim Finkle, *FBI warns healthcare firms that they are targeted by hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-byhackers-idUSKBN0GK24U20140820.

[28] Nathan Eddy, *2025's Biggest Healthcare Cybersecurity Threats*, HEALTHTECH (Jan. 24, 2025), https://healthtechmagazine.net/article/2025/01/healthcare-cybersecurity-threats-2025-perfcon#:~:text=A%20recent%20report%20from%20Proofpoint%20found%2092%,the%20most%20expensive%20attack%20was%20$4.7%20million.

[29] Jill McKeon, *Biggest Healthcare Data Breaches Reported This Year, So Far,* HEALTHTECH SECURITY (June 26, 2023), https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far.

82. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendants.

Defendants Failed to Comply with FTC Guidelines

83. 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.

84. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[30] 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.[31]

85. 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 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.

[30] FED. TRADE COMM'N, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[31] *Id*.

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

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

88. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices.

89. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' and employees' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

90. Defendants were at all times fully aware of their obligation to protect the Private Information of their patients and employees. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Industry Standards

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

92. 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.[32]

93. 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.

[32] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited June 3, 2025).

94. 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 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.[33]

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

[33] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited June 3, 2025).

Defendants Failed to Comply with HIPAA's Requirements

96. HIPAA requires covered entities such as Defendants to protect against reasonably anticipated threats to the security of Protected Health Information ("PHI").

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

98. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

99. A Data Breach such as the one Defendants experienced is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information."

See 45 C.F.R. 164.402.

100. Defendants' Data Breach resulted from a combination of insufficiencies that indicate Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards. It can be inferred from the Data Breach that Defendants either failed to

implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' Private Information, including PHI.

101. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

102. 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."

103. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

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

105. 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.

106. 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.

107. 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.

108. 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.

109. The Data Breach could have been prevented if Defendants had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored their obligations to their patients and employees.

Defendants Breached Their Duties and Obligations to Plaintiffs and the Class

110. Defendants breached duties and obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and their patients' and employees' data.

111. The Private Information impacted in the Data Breach was maintained on Excelsior's computer network in a way that left it vulnerable to cybersecurity attacks. At set forth above, data breaches impacting healthcare providers and networks are a known risk to Defendants, and Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left the data vulnerable to an attack.

112. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cybersecurity attacks;
b. Failing to adequately protect employees', patients', and other affiliated persons' Private Information;
c. Failing to properly monitor their own data security systems for existing intrusions;
d. Failing to utilize industry standard data security protections;
e. Failing to timely notify Plaintiffs and Class Members of the Data Breach;

f. Failing to ensure the confidentiality and integrity of the electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

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

l. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of Defendants' workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

n. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

113. As the result of maintaining their computer systems in a manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

114. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased and imminent risk of fraud and identity theft.

Data Breaches Put Consumers and Employees at an Increased Risk of Fraud, Identify Theft, and Other Harms

115. Data breaches such as the one outlined herein are especially problematic because of the disruption they cause to the overall daily lives of victims affected.

116. A data breach naturally increases the risk to an individual of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other

miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[34]

117. Individuals are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing a person's identity and is likened to accessing your DNA for hacker's purposes.

118. Data breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers.

119. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[35]

120. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

121. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[36] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for

[34] Erika Harrell, *Victims of Identity Theft, 2018* (April 2021), NCJ 256085 at 9, BUREAU OF JUST. STAT., U.S. DEP'T OF JUST., https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.
[35] *Identity Theft and Your Social Security Numbers* (July 2021), SOCIAL SECURITY ADMINISTRATION, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 3, 2025).
[36] *Id.*

unemployment benefits, or apply for a job using a false identity.[37] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number 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.

122. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security numbers to obtain government benefits; or file a fraudulent tax return using the victim's information.

123. Moreover, it is not an 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. Even then, a new Social Security number may not be effective, as "[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."[38]

124. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of Private Information in its 2023 Consumer Impact Report.[39] 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;

[37] *Id.*
[38] Brian 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-millions-worrying-about-identity-theft.
[39] *2023 Consumer Impact Report* (Aug. 2023), IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (last visited June 3, 2025).

- 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.[40]

125. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the GAO, which has conducted studies 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.[41]

126. Theft of Private Information is even more harmful when it includes PHI. 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.[42]

---

[40] *Id*. at pp 21-25.

[41] *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*, at 2 (June 2007), https://www.gao.gov/products/gao-07-737.

[42] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

127. 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. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[43]

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

The Steps Victims Must Take to Protect Themselves Cost Significant Time and Money

129. Once Private Information is stolen, it costs significant time and/or money to attempt to protect one's identity.

130. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps victims can take after a data breach.[44] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the victims' options. It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiffs and Class Members) must take after this Data Breach are both time-consuming and of limited and short-term effectiveness.

---

[43] *Id*.

[44] U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-230, *Report to Congressional Requestors: Range of Consumer Risks Highlights Limitations of Identify Theft Services* (Mar. 2019), https://www.gao.gov/assets/gao-19-230.pdf.

131. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record," discussing the same in a 2007 report as well ("2007 GAO Report").[45]

132. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 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.[46]

133. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

134. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

Private Information Is Inherently Valuable

135. Private Information is a valuable property right.[47]

---

[45] GAO Report, n.41, *supra*.
[46] *See What to Do Right Away,* FED. TRADE COMM'N, https://www.identitytheft.gov/Steps (last visited June 3, 2025).
[47] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

136. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering."[48]

137. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[49]

138. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[50]

139. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendants therefore knew or should have known this and strengthened their data systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

140. Here, not only was sensitive medical information compromised, but financial information and Social Security numbers were compromised too. The value of Private Information, including PHI, is axiomatic. The value of "big data" in corporate America is

[48] *A Cost Analysis of Healthcare Sector Data Breaches,* U.S. DEP'T HEALTH & HUMAN SERVS., at 2 (Apr. 12, 2019), available at https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf.
[49] *5 Important Elements to Establish Data Security in Healthcare,* ADVENTHEALTH UNIVERSITY BLOG (May 21, 2020), https://www.ahu.edu/blog/data-security-in-healthcare.
[50] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, COMPUTER WORLD (Feb. 6, 2015), https://www.networkworld.com/article/935334/ anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

141. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade it on the dark web for years.

142. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

The Private Information Disclosed During the Data Breach Has Been Disseminated on the Dark Web

143. MONTI—the cybercriminal group that carried out the Data Breach—operates as a ransomware group, targeting large and small organizations, exfiltrating sensitive information and medical images, and publishing the stolen data on its dark web blog and selling it on the black market.[51]

144. In the summer of 2024, MONTI claimed to hack Defendants' servers and computer systems, thereby gaining access to the Private Information of Defendants' patients and employees.[52]

145. According to MONTI, once they gained control over Defendants' servers, they exfiltrated approximately 300 gigabytes of patient and employee data and immediately threatened to publish the compromised Private Information on the dark web.[53]

---

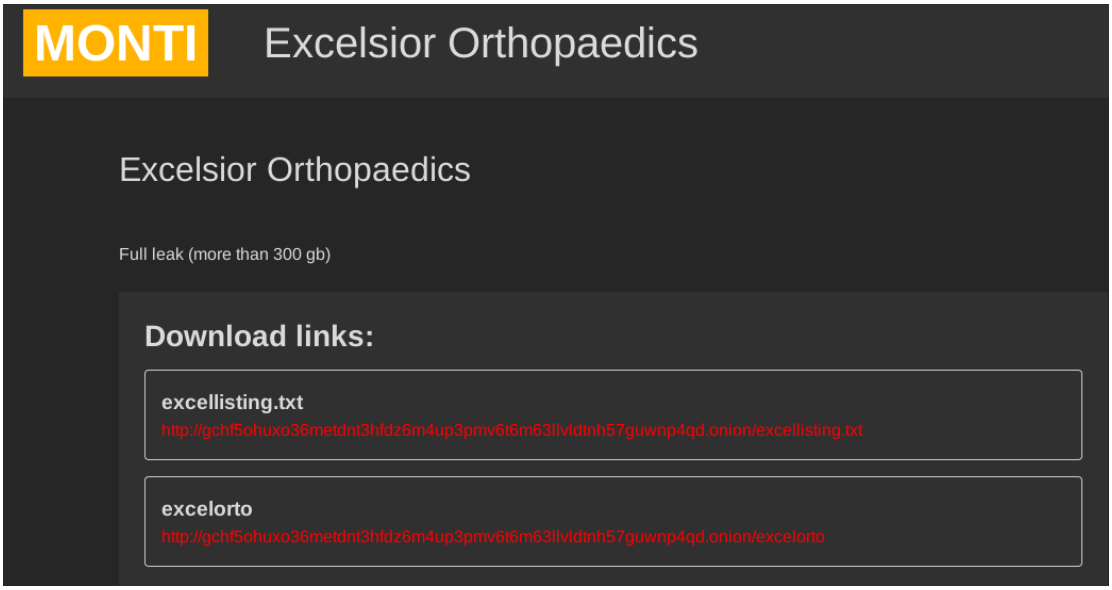
[51] Dryna Antoniuk, *Monti ransomware targets legal and gov't entities with new Linux-based variant*, THE RECORD (Aug. 16, 2023), https://therecord.media/monti-ransomware-targets-govt-entities; *Monti Ransomware*, AVERTIUM (Sept. 12, 2023), https://www.avertium.com/resources/threat-reports/monti-ransomware.

[52] Samiksha Jain, *MONTI Ransomware Targets New York Orthopaedic Center Excelsior Orthopaedics*, THE CYBER EXPRESS (July 9, 2024), https://thecyberexpress.com/monti-ransomware-attack-excelsior-orthopaedics/.

[53] Ionut Arghire, *Excelsior Orthopaedics Data Breach Impacts 357,000 People*, SECURITYWEEK (Jan. 9, 2025), https://www.securityweek.com/excelsior-orthopaedics-data-breach-impacts-357000-people/.

146. On or around July 16, 2024, MONTI's threats became reality, as the data was publicly posted on MONTI's Tor-based dark web leak site.[54] The MONTI Tor site remained active through January 23, 2025, with "Excelsior Orthopaedics" listed among the companies impacted. A screenshot showing the Excelsior Orthopaedics listing, the 300-gigabyte size of exfiltrated data, and associated download links on MONTI's leak site is shown in Figure 1 below.

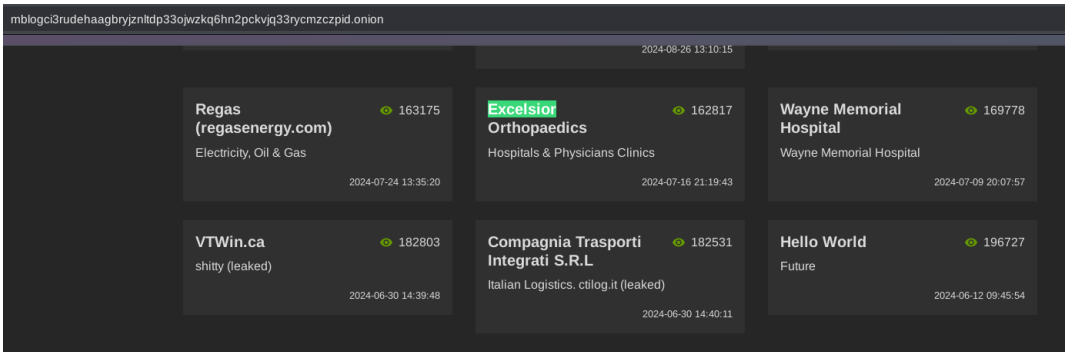
Figure 1



147. The Excelsior data set was confirmed to be available for download via multiple Tor-based links, with the relevant breach page showing over 162,000 views, thereby evidencing widespread and ongoing access to the compromised information. A screenshot of the Excelsior Orthopaedics entry—displayed alongside listings for other breached companies and showing the view count as of January 23, 2025—is shown in Figure 2 below.

[54] Jain, n.52, *supra*.

Figure 2



148. Screenshots and archived copies of the MONTI leak site confirm that Plaintiffs' and Class Members' data remains accessible to third parties, including identity thieves, fraudsters, data brokers, and other malicious actors.

149. And as set forth above and confirmed through expert review of the dark web, the data exfiltrated from Defendants' systems by MONTI includes highly sensitive personal, medical, and professional information and images belonging to Plaintiffs and Class Members, such as full names, addresses, dates of birth, Social Security numbers, driver's license numbers, non-driver identification card numbers, biometric information, medical test documentation, and the like.

150. Specific examples of such compromised information include the following subsets, which are also visually documented with appropriate redaction in **Exhibit A** attached hereto:

a. Photographs of American passports and Social Security cards;

b. State-issued identification cards;

c. Medical imaging, such as X-rays revealing diagnostic conditions (*e.g.*, Apophysitis—an overuse injury affecting growth plates in children and adolescents);[55]

[55] Due to the sensitive and personal nature of the compromised images at issue, and out of respect for the victims to whom such images belong, Plaintiffs have elected not to include exemplars of them publicly at this time as part of

d. Controlled Substance Registration Certificates issued by the U.S. Drug Enforcement Administration (DEA);

e. Employee onboarding documents and provider credentialing forms containing National Provider Identifier (NPI) numbers; council for Affordable Quality Healthcare (CAQH) numbers; workers' compensation claim numbers; personal cell phone numbers; dates of birth; and state medical license numbers (e.g., NYS License); DEA registration numbers; Medicaid provider IDs; and educational background, including undergraduate institution, medical school, and residency program.

151. This type of data is extremely sensitive and, in many cases, permanent or irreplaceable. Its exposure presents a serious and ongoing risk of identity theft, fraud, and reputational harm.

152. Indeed, a forensic analysis of Defendants' data environment, which was conducted using commercially available Private Information detection software, revealed the widespread and unsecured storage of highly sensitive personal and medical information across 57.1 gigabytes of data exfiltrated on the dark web from Defendants' systems. The scan detected and categorized large volumes of protected data typically safeguarded under federal and state privacy laws.

153. Specifically, the scan identified tens of thousands of files containing Private Information, including but not limited to:

a. Over 32,000 dates of birth;

b. Over 36,000 email addresses;

c. Over 112,000 phone numbers;

Exhibit A. However, if the Court determines that the inclusion of such images is necessary, Plaintiffs will file the images with the Court under seal.

d. Over 160,000 street address entries;

e. Over 10,000 bank account records;

f. Sensitive health and medical data, including sensitive imaging/X-rays, in more than 7,500 files;

g. Passwords stored in nearly 100 files;

h. Government-issued ID scans and photographic facial images;

i. Files reflecting sensitive attributes such as race, religion, and sexual orientation;

j. Over 1,300 Social Security numbers and multiple instances of passport-related information.

154. These records appeared across a diverse array of document formats, including PDFs, Word and Excel files, image files (e.g., JPG, PNG, TIFF), emails, and credentialing documents—indicating that Defendants maintained this data in an unstructured, decentralized, and improperly managed fashion.

155. The scale, nature, and distribution of this Private Information—stored without evidence of meaningful encryption, data segmentation, or access controls—demonstrates that Defendants failed to implement reasonable and industry-standard safeguards for the protection of personal and health information. This systemic failure constitutes a violation of applicable data protection laws and supports Plaintiffs' claims that Defendants acted negligently and with disregard for the security of individuals' most private data.

156. The MONTI leak was not the only vector through which Plaintiffs' and Class Members' data became publicly accessible. The compromised data—particularly email credentials and associated personal identifiers—have propagated across multiple cybercrime platforms, including historic breach aggregators, dark web indexes, and credential marketplaces.

157. For example, the dark web forum BreachForums, a known marketplace for trafficking stolen datasets, currently hosts the Pureincubation leak, which includes compromised email addresses tied to Excelsior. While not labeled explicitly as an Excelsior leak, many of the records within the Pureincubation database correspond to Excelsior's corporate email domains and naming conventions.

158. Cyber threat investigators using the platform NexusXplore identified approximately 773 Excelsior-associated credentials previously exposed in data breaches across various platforms. A large portion of these records included unencrypted (clear text) passwords.

159. The breach aggregation website LeakPeak.com identified 107 additional credential entries tied to Excelsior Orthopaedics email accounts, many of which appeared in datasets from more recent breaches of popular consumer services, including Omaze.com, ShareThis.com, MyFitnessPal.com, HomeChef.com, and Verifications.io. These credentials also included clear text passwords.

160. The dark web indexing site Ransomlook.io, which archives and displays ransomware group leak sites, corroborated the timeline of MONTI's publication by displaying a screenshot of the Excelsior Orthopaedics listing on the MONTI Tor site. The listing noted a scheduled release date of July 16, 2024, and had accumulated at least 846 public views as of that month, indicating widespread circulation and public indexing of the stolen data.

161. The continued appearance of Excelsior-related credentials and identifiers on these illicit platforms—months after the initial leak—demonstrates that Defendants' security failures have resulted not only in a one-time breach but in an ongoing, uncontrolled dissemination of private, sensitive, and exploitable data across multiple criminal ecosystems.

PLAINTIFFS' EXPERIENCES

Plaintiff Susan Szucs

162. On or about December 31, 2024, Plaintiff Szucs received a Notice of Data Security Incident, notifying Plaintiff that her Private Information may have been exposed in the Data Breach.

163. Plaintiff Szucs received medical or related services from Excelsior. As a condition of receiving those services, Excelsior required Plaintiff—or a third party acting on Plaintiff's behalf—to provide Plaintiff's Private Information.

164. Based on representations made by Defendants, Plaintiff Szucs believed Defendants implemented and maintained reasonable security to protect her Private Information.

165. At the time of the Data Breach, Defendants maintained Plaintiff's Private Information in their systems.

166. Plaintiff Szucs is very careful about sharing sensitive Private Information. Plaintiff Szucs stores any documents containing Private Information in a safe and secure location. Plaintiff Szucs has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Szucs diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her, Plaintiff Szucs uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

167. Plaintiff Szucs is alarmed by the breadth of information involved in the Data Breach, especially since Defendants failed to notify her of any issue for close to six months. During that time period, Plaintiff Szucs' Private Information was in the hands of cybercriminals and Plaintiff was given no notice to take steps to try and protect herself.

168. Defendants failed to notify Plaintiff Szucs of any issue for close to six months. During that time period, Plaintiff's Private Information was in the hands of cybercriminals and Plaintiff Szucs was given no notice to take steps to try and protect herself.

169. Plaintiff Szucs would not have accepted services from Excelsior and would not have provided Private Information to Defendants (or agreed to have Defendants receive Private Information), had Plaintiff known that her Private Information would not be adequately safeguarded by Defendants, or had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their patients' personal and health information from theft, and that those systems were subject to a data breach.

170. Plaintiff Szucs made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching and verifying the legitimacy of the Data Breach upon receiving the Notice and monitoring accounts for any indication of fraudulent activity. Plaintiff Szucs has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

171. Plaintiff Szucs' Private Information has already been stolen and misused as evidenced by the fact that she experienced incidents of fraud and identity theft in the form of unauthorized charges to her checking account. Plaintiff Szucs had to contact the bank to get the charge reversed and cancel her debit card. These actions by third parties have detrimentally impacted Plaintiff Szucs' life as a whole and specifically caused financial strain on her as a direct result of the Data Breach.

172. Plaintiff Szucs suffered actual injury from having Private Information compromised as a result of the Data Breach, including, but not limited to: (i) theft of Private

Information; (ii) lost or diminished value of Private Information; (iii) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to Plaintiff's Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

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

174. The Data Breach has also caused Plaintiff Szucs to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

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

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

Plaintiff Anthony Parrizzi

177. On or about December 31, 2024, Plaintiff Parrizzi received a Notice of the Data Breach, notifying Plaintiff that his Private Information may have been exposed in the Data Breach.

178. Plaintiff Parrizzi received medical or related services from Excelsior. As a condition of receiving those services, Excelsior required Plaintiff Parrizzi —or a third party acting on his behalf—to provide Plaintiff's Private Information.

179. Based on representations made by Defendants, Plaintiff Parrizzi believed Defendants implemented and maintained reasonable security to protect his Private Information.

180. At the time of the Data Breach, Defendants maintained Plaintiff Parrizzi's Private Information in their systems.

181. Plaintiff Parrizzi is very careful about sharing sensitive Private Information. Plaintiff Parrizzi stores any documents containing Private Information in a safe and secure location. Plaintiff Parrizzi has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Parrizzi diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him, Plaintiff Parrizzi uses two-factor or multifactor authentication to add an extra layer of security to his Private Information

182. Plaintiff Parrizzi is especially alarmed by the breadth of information involved in the Data Breach. However, even worse for Plaintiff, the Notice did not specify what "medical information" or "health insurance" information was exposed and failed to notify him of any issue for close to six months. During that time period, Plaintiff Parrizzi's Private Information was in the hands of cybercriminals and he was given no notice to take steps to try and protect himself.

183. Plaintiff Parrizzi would not have accepted services from Excelsior and would not have provided Private Information to Defendants (or agreed to have Defendants receive Private Information), had he known that his Private Information would not be adequately safeguarded by Defendants, or had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their patients' personal and health information from theft, and that those systems were subject to a Data Breach.

184. Plaintiff Parrizzi made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching and verifying the legitimacy of the Data Breach upon receiving the Notice and monitoring accounts for any indication of fraudulent activity. Plaintiff Parrizzi has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

185. Plaintiff Parrizzi's Private Information has already been stolen and misused as evidenced by the fact that he experienced incidents of fraud and identity theft in the form of notifications that his information is available on the dark web and an increase in spam calls since the Data Breach. These actions by third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

186. Plaintiff Parrizzi suffered actual injury from having Private Information compromised as a result of the Data Breach, including, but not limited to: (i) theft of Private Information; (ii) lost or diminished value of Private Information; (iii) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and

certainly increased risk to Plaintiff's Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

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

188. The Data Breach has also caused Plaintiff Parrizzi to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

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

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

Plaintiff Terrence Ernest Giddy

191. On or about December 31, 2024, Plaintiff Giddy received a Notice of the Data Breach, notifying him that his Private Information may have been exposed in the Data Breach.

192. Plaintiff Giddy received medical or related services from Excelsior. As a condition of receiving those services, Excelsior required Plaintiff Giddy—or a third party acting on his behalf—to provide his Private Information.

193. Based on representations made by Defendants, Plaintiff Giddy believed Defendants implemented and maintained reasonable security to protect his Private Information.

194. At the time of the Data Breach, Defendants maintained Plaintiff Giddy's Private Information in their systems.

195. Plaintiff Giddy is very careful about sharing sensitive Private Information. Plaintiff Giddy stores any documents containing Private Information in a safe and secure location. Plaintiff Giddy has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Giddy diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him, Plaintiff Giddy uses two-factor or multifactor authentication to add an extra layer of security to his Private Information

196. Plaintiff Giddy is especially alarmed by the breadth of information involved in the Data Breach. However, even worse for Plaintiff Giddy, the Notice did not specify what "medical information" or "health insurance" information was exposed, and failed to notify him of any issue for close to six months. During that time period, Plaintiff Giddy's Private Information was in the hands of cybercriminals and he was given no notice to take steps to try and protect himself.

197. Plaintiff Giddy would not have accepted services from Excelsior and would not have provided Private Information to Defendants (or agreed to have Defendants receive Private Information), had he known that his Private Information would not be adequately safeguarded by Defendants, or had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their patients' personal and health information from theft, and that those systems were subject to a Data Breach.

198. Plaintiff Giddy made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching and verifying the legitimacy of the Data Breach upon receiving the Notice and monitoring accounts for any indication of fraudulent activity. Plaintiff Giddy has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

199. Plaintiff Giddy's Private Information has already been stolen and misused as evidenced by the fact that he experienced incidents of fraud and identity theft in the form of fraudulent charges to his accounts and an increase in spam since the Data Breach. These actions by third parties have detrimentally impacted Plaintiff Giddy's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

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

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

202. The Data Breach has also caused Plaintiff Giddy to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

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

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

Plaintiff Christina Church

205. On or about December 31, 2024, Plaintiff Church received a Notice of the Data Breach, notifying her that her Private Information may have been exposed in the Data Breach.

206. Plaintiff Church received medical or related services from Excelsior. As a condition of receiving those services, Excelsior required Plaintiff Church—or a third party acting on her behalf—to provide her Private Information.

207. Based on representations made by Defendants, Plaintiff Church believed Defendants implemented and maintained reasonable security to protect her Private Information.

208. At the time of the Data Breach, Defendants maintained Plaintiff Church's Private Information in their systems.

209. Plaintiff Church is very careful about sharing sensitive Private Information. Plaintiff Church stores any documents containing Private Information in a safe and secure location. Plaintiff Church has never knowingly transmitted unencrypted sensitive Private Information over

the internet or any other unsecured source. Moreover, Plaintiff Church diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her, Plaintiff Church uses two-factor or multifactor authentication to add an extra layer of security to her Private Information

210. Plaintiff Church is especially alarmed by the breadth of information involved in the Data Breach. However, even worse for Plaintiff Church, the Notice did not specify what "medical information" or "health insurance" information was exposed, and failed to notify her of any issue for close to six months. During that time period, Plaintiff Church's Private Information was in the hands of cybercriminals and she was given no notice to take steps to try and protect herself.

211. Plaintiff Church would not have accepted services from Excelsior and would not have provided Private Information to Defendants (or agreed to have Defendants receive Private Information), had she known that her Private Information would not be adequately safeguarded by Defendants, or had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their patients' personal and health information from theft, and that those systems were subject to a Data Breach.

212. Plaintiff Church made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching and verifying the legitimacy of the Data Breach upon receiving the Notice and monitoring accounts for any indication of fraudulent activity. Plaintiff Church has spent significant time dealing with the Data Breach—valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

213. Plaintiff Church's Private Information has already been stolen and misused as evidenced by the fact that she experienced incidents of fraud and identity theft in the form of suspicious transactions on her accounts, her information being found on the dark web, someone opening a credit account in her name, and an increase in spam since the Data Breach. These actions by third parties have detrimentally impacted Plaintiff Church's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

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

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

216. The Data Breach has also caused Plaintiff Church to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

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

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

Plaintiff Jimmy Hardaway, Jr.

219. On or about December 31, 2024, Plaintiff Hardaway received a Notice of the Data Breach, notifying him that his Private Information may have been exposed in the Data Breach.

220. Plaintiff Hardaway received medical or related services from Excelsior. As a condition of receiving those services, Excelsior required Plaintiff Hardaway—or a third party acting on his behalf—to provide his Private Information.

221. Based on representations made by Defendants, Plaintiff Hardaway believed Defendants implemented and maintained reasonable security to protect his Private Information.

222. At the time of the Data Breach, Defendants maintained Plaintiff Hardaway's Private Information in their systems.

223. Plaintiff Hardaway is very careful about sharing sensitive Private Information. Plaintiff Hardaway stores any documents containing Private Information in a safe and secure location. Plaintiff Hardaway has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Hardaway diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available

to him, Plaintiff Hardaway uses two-factor or multifactor authentication to add an extra layer of security to his Private Information

224. Plaintiff Hardaway is especially alarmed by the breadth of information involved in the Data Breach. However, even worse for Plaintiff Hardaway, the Notice did not specify what "medical information" or "health insurance" information was exposed, and failed to notify him of any issue for close to six months. During that time period, Plaintiff Hardaway's Private Information was in the hands of cybercriminals and Plaintiff Hardaway was given no notice to take steps to try and protect himself.

225. Plaintiff Hardaway would not have accepted services from Excelsior and would not have provided Private Information to Defendants (or agreed to have Defendants receive Private Information), had he known that his Private Information would not be adequately safeguarded by Defendants, or had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their patients' personal and health information from theft, and that those systems were subject to a Data Breach.

226. Plaintiff Hardaway made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching and verifying the legitimacy of the Data Breach upon receiving the Notice and monitoring accounts for any indication of fraudulent activity. Plaintiff Hardaway has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

227. Plaintiff Hardaway's Private Information has already been stolen and misused as evidenced by the fact that he experienced incidents of fraud and identity theft in the form of increase in spam since the Data Breach. These actions by third parties have detrimentally impacted

Plaintiff Hardaway's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

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

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

230. The Data Breach has also caused Plaintiff Hardaway to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

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

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

Plaintiff Sharon Siegle

233. On or about December 31, 2024, Plaintiff Siegle received a Notice of the Data Breach, notifying her that her Private Information may have been exposed in the Data Breach.

234. Plaintiff Siegle received medical or related services from Excelsior. As a condition of receiving those services, Excelsior required Plaintiff Siegle—or a third party acting on her behalf—to provide her Private Information.

235. Based on representations made by Defendants, Plaintiff Siegle believed Defendants implemented and maintained reasonable security to protect her Private Information.

236. At the time of the Data Breach, Defendants maintained Plaintiff Siegle's Private Information in their systems.

237. Plaintiff Siegle is very careful about sharing sensitive Private Information. Plaintiff Siegle stores any documents containing Private Information in a safe and secure location. Plaintiff Siegle has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Siegle diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her, Plaintiff Siegle uses two-factor or multifactor authentication to add an extra layer of security to her Private Information

238. Plaintiff Siegle is especially alarmed by the breadth of information involved in the Data Breach. However, even worse for Plaintiff Siegle, the Notice did not specify what "medical information" or "health insurance" information was exposed, and failed to notify her of any issue

for close to six months. During that time period, Plaintiff Siegle's Private Information was in the hands of cybercriminals and she was given no notice to take steps to try and protect herself.

239. Plaintiff Siegle would not have accepted services from Excelsior and would not have provided Private Information to Defendants (or agreed to have Defendants receive Private Information), had she known that her Private Information would not be adequately safeguarded by Defendants, or had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their patients' personal and health information from theft, and that those systems were subject to a Data Breach.

240. Plaintiff Siegle made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching and verifying the legitimacy of the Data Breach upon receiving the Notice and monitoring accounts for any indication of fraudulent activity. Plaintiff Siegle has spent significant time dealing with the Data Breach—valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

241. Plaintiff Siegle's Private Information has already been stolen and misused as evidenced by the fact that she experienced incidents of fraud and identity theft in the form of increase in spam calls, including a death threat, notices of her information being on the dark web, a drop in her credit score due to an unauthorized inquiry, and an unauthorized attempt to use her credit card in another state since the Data Breach. These actions by third parties have detrimentally impacted Plaintiff Siegle's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

242. Plaintiff Siegle suffered actual injury from having Private Information compromised as a result of the Data Breach, including, but not limited to: (i) theft of Private

Information; (ii) lost or diminished value of Private Information; (iii) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to Plaintiff's Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

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

244. The Data Breach has also caused Plaintiff Siegle to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

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

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

Plaintiff Paul Pascucci

247. On or about December 31, 2024, Plaintiff Pascucci received a Notice of the Data Breach, notifying Plaintiff that his Private Information may have been exposed in the Data Breach.

248. Plaintiff Pascucci received medical or related services from Excelsior. As a condition of receiving those services, Excelsior required Plaintiff Pascucci—or a third party acting on his behalf—to provide his Private Information.

249. Based on representations made by Defendants, Plaintiff Pascucci believed Defendants implemented and maintained reasonable security to protect his Private Information.

250. At the time of the Data Breach, Defendants maintained Plaintiff Pascucci's Private Information in their systems.

251. Plaintiff Pascucci is very careful about sharing sensitive Private Information. Plaintiff Pascucci stores any documents containing Private Information in a safe and secure location. Plaintiff Pascucci has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Pascucci diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him, Plaintiff Pascucci uses two-factor or multifactor authentication to add an extra layer of security to his Private Information

252. Plaintiff Pascucci is especially alarmed by the breadth of information involved in the Data Breach. However, even worse for Plaintiff Pascucci, the Notice did not specify what "medical information" or "health insurance" information was exposed, and failed to notify him of any issue for close to six months. During that time period, Plaintiff Pascucci's Private Information was in the hands of cybercriminals and he was given no notice to take steps to try and protect himself.

253. Plaintiff Pascucci would not have accepted services from Excelsior and would not have provided Private Information to Defendants (or agreed to have Defendants receive Private Information), had he known that his Private Information would not be adequately safeguarded by Defendants, or had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their patients' personal and health information from theft, and that those systems were subject to a Data Breach.

254. Plaintiff Pascucci made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching and verifying the legitimacy of the Data Breach upon receiving the Notice and monitoring accounts for any indication of fraudulent activity. Plaintiff Pascucci has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

255. Plaintiff Pascucci's Private Information has already been stolen and misused as evidenced by the fact that he experienced incidents of fraud and identity theft in the form of the credit card he used with Excelsior being compromised, info found on the dark web by McAfee, and an increase in spam since the Data Breach. These actions by third parties have detrimentally impacted Plaintiff Pascucci's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

256. Plaintiff Pascucci suffered actual injury from having Private Information compromised as a result of the Data Breach, including, but not limited to: (i) theft of Private Information; (ii) lost or diminished value of Private Information; (iii) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences

of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to Plaintiff's Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

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

258. The Data Breach has also caused Plaintiff Pascucci to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

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

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

Plaintiff James Marciszewski

261. On or about December 31, 2024, Plaintiff Marciszewski received a Notice of the Data Breach, notifying him that his Private Information may have been exposed in the Data Breach.

262. Plaintiff Marciszewski received medical or related services from Excelsior. As a condition of receiving those services, Excelsior required Plaintiff Marciszewski—or a third party acting on his behalf—to provide his Private Information.

263. Based on representations made by Defendants, Plaintiff Marciszewski believed Defendants implemented and maintained reasonable security to protect his Private Information.

264. At the time of the Data Breach, Defendants maintained Plaintiff Marciszewski's Private Information in their systems.

265. Plaintiff Marciszewski is very careful about sharing sensitive Private Information. Plaintiff Marciszewski stores any documents containing Private Information in a safe and secure location. Plaintiff Marciszewski has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Marciszewski diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him, Plaintiff Marciszewski uses two-factor or multifactor authentication to add an extra layer of security to his Private Information

266. Plaintiff Marciszewski is especially alarmed by the breadth of information involved in the Data Breach. However, even worse for Plaintiff Marciszewski, the Notice did not specify what "medical information" or "health insurance" information was exposed, and failed to notify him of any issue for close to six months. During that time period, Plaintiff Marciszewski's Private Information was in the hands of cybercriminals and he was given no notice to take steps to try and protect himself.

267. Plaintiff Marciszewski would not have accepted services from Excelsior and would not have provided Private Information to Defendants (or agreed to have Defendants receive Private

Information), had he known that his Private Information would not be adequately safeguarded by Defendants, or had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their patients' personal and health information from theft, and that those systems were subject to a Data Breach.

268. Plaintiff Marciszewski made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching and verifying the legitimacy of the Data Breach upon receiving the Notice and monitoring accounts for any indication of fraudulent activity. Plaintiff Marciszewski has spent significant time dealing with the Data Breach—valuable time he otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

269. Plaintiff Marciszewski's Private Information has already been stolen and misused as evidenced by the fact that he experienced incidents of fraud and identity theft in the form of his Citi Mastercard being compromised in February of 2025 resulting in unauthorized charges, as well as an increase in spam since the Data Breach. These actions by third parties have detrimentally impacted Plaintiff Marciszewski's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

270. Plaintiff Marciszewski suffered actual injury from having Private Information compromised as a result of the Data Breach, including, but not limited to: (i) theft of Private Information; (ii) lost or diminished value of Private Information; (iii) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to Plaintiff's Private Information, which: (a) remains unencrypted and

available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

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

272. The Data Breach has also caused Plaintiff Marciszewski to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

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

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

Plaintiff Shannon Allgrim

275. On or about December 31, 2024, Plaintiff Allgrim received a Notice of the Data Breach, notifying her that her Private Information may have been exposed in the Data Breach.

276. Plaintiff Allgrim received medical or related services from Excelsior. As a condition of receiving those services, Excelsior required Plaintiff Allgrim—or a third party acting on her behalf—to provide her Private Information.

277. Based on representations made by Defendants, Plaintiff Allgrim believed Defendants implemented and maintained reasonable security to protect her Private Information.

278. At the time of the Data Breach, Defendants maintained Plaintiff Allgrim's Private Information in their systems.

279. Plaintiff Allgrim is very careful about sharing sensitive Private Information. Plaintiff Allgrim stores any documents containing Private Information in a safe and secure location. Plaintiff Allgrim has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Allgrim diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her, Plaintiff Allgrim uses two-factor or multifactor authentication to add an extra layer of security to her Private Information

280. Plaintiff Allgrim is especially alarmed by the breadth of information involved in the Data Breach. However, even worse for Plaintiff Allgrim, the Notice did not specify what "medical information" or "health insurance" information was exposed, and failed to notify her of any issue for close to six months. During that time period, Plaintiff Allgrim's Private Information was in the hands of cybercriminals and she was given no notice to take steps to try and protect herself.

281. Plaintiff Allgrim would not have accepted services from Excelsior and would not have provided Private Information to Defendants (or agreed to have Defendants receive Private Information), had she known that her Private Information would not be adequately safeguarded by Defendants, or had Defendants timely disclosed that their systems lacked adequate computer and

data security practices to safeguard their patients' personal and health information from theft, and that those systems were subject to a Data Breach.

282. Plaintiff Allgrim made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching and verifying the legitimacy of the Data Breach upon receiving the Notice and monitoring accounts for any indication of fraudulent activity. Plaintiff Allgrim has spent significant time dealing with the Data Breach—valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

283. Plaintiff Allgrim's Private Information has already been stolen and misused as evidenced by the fact that she received a fraud alert from her bank after unauthorized charge on her account, notices of her information being on the dark web, an unauthorized car loan being taken out in her name and appearing on her credit report, and an increase in spam since the Data Breach. These actions by third parties have detrimentally impacted Plaintiff Allgrim's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

284. Plaintiff Allgrim suffered actual injury from having Private Information compromised as a result of the Data Breach, including, but not limited to: (i) theft of Private Information; (ii) lost or diminished value of Private Information; (iii) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to Plaintiff's Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in

Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

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

286. The Data Breach has also caused Plaintiff Allgrim to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

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

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

PLAINTIFFS' AND CLASS MEMBERS' INJURIES

289. To date, Defendants have done nothing to compensate Plaintiffs and Class Members for the damages they sustained in the Data Breach.

290. Defendants have merely offered credit monitoring services. Defendants' limited offer is inadequate as victims are likely to face many years of identity theft and/or are facing circumstances where they are substantially certain to be exposed to identity theft and attendant harms.

291. Defendants' offer fails to compensate victims of the Data Breach—who now face an indefinite risk of identity theft—for the unauthorized release and disclosure of Private Information, out-of-pocket costs, and time spent attempting to mitigate their injuries.

292. Furthermore, Defendants' credit monitoring offer and suggestions for how to handle the fallout of the Data Breach squarely place the burden on Plaintiffs and Class Members, rather than on the Defendants, to investigate and protect themselves from the Data Breach.

293. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their Private Information, and by the disruption to their lives as a direct and foreseeable consequence of the Data Breach.

294. Plaintiffs and Class Members were damaged in that their Private Information is now in the hands of cybercriminals, sold and potentially for sale for years into the future.

295. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

296. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

297. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans and credit accounts fraudulently opened in their names, unauthorized charges on financial accounts, personal and medical information disclosed on the dark web, decreases in credit scores, and other identity theft in addition to the actual fraud and identity theft that has already occurred. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

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

299. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyberthieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

300. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

301. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

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

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

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

g. Placing “freezes” and “alerts” with credit reporting agencies;

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

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

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

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

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

302. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information as well as health information is not accessible online and that access to such data is password-protected.

303. Further, as a result of Defendants' conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

304. Defendants' delay in identifying and reporting the Data Breach exacerbated its harm. In a data breach, time is of the essence to reduce the imminent misuse of Private Information. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Excelsior knew the breach began in June 2024 but did not begin notifying the victims until August 2024, with the majority of affected individuals not receiving notice until December 31, 2024. Yet, Defendants

offered no explanation for the delay. This delay violates HIPAA and other notification requirements and increased the injuries to Plaintiffs and Class Members.

CLASS ACTION ALLEGATIONS

305. Plaintiffs bring this action individually and on behalf of all other persons similarly situated under CPLR 901, *et seq.*

306. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class:**
> All persons residing in the United States whose Private Information was compromised as a result of the Data Breach, including all persons who received notice of the breach.
>
> **New York Class:**
> All persons residing in the State of New York whose Private Information was compromised as a result of the Data Breach, including all persons who received notice of the breach.

307. Excluded from the Classes are Defendants' officers and directors; any entity in which Defendants have a controlling interest; the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants; and members of the judiciary to whom this case is assigned, their families, and members of their staff.

308. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification

309. Numerosity, CPLR § 901(a)(1): The Class Members are so numerous that joinder of all of them is impracticable. The exact number of Class Members is currently unknown, but believed to be approximately 357,000.

310. Commonality. As required by CPLR § 901(a)(2), there are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

f. Whether Defendants breached their duties to Plaintiffs and Class Members to safeguard their Private Information;

g. Whether unauthorized third parties obtained Plaintiffs' and Class Members' Private Information in the Data Breach;

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

i. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

j. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

k. Whether Defendants' conduct violated the FTCA, HIPAA, industry standards, and/or New York General Business Law § 349;

l. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

m. Whether Defendants' conduct was negligent or negligent per se;

n. Whether there was an actual or implied contract, between Defendants on one hand and Plaintiffs and Class Members on the other, requiring Defendants to adequately protect Plaintiffs' and Class Members' Private Information;

o. Whether Defendants breached any such contract;

p. Whether Defendants had a fiduciary duty to protect Plaintiffs' and Class Members' Private Information;

q. Whether Defendants breached their fiduciary duty;

r. Whether Defendants were unjustly enriched; and

s. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

311. Typicality, CPLR § 901(a)(3): Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

312. Adequacy of Representation, CPLR § 901(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

313. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

314. Superiority, CPLR § 901(a)(5): A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

315. Defendants have acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a classwide basis. Further, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, is encrypted, and is password protected. Damages from a

future breach due to Defendants' inadequate data security represent an irreparable injury (such as the further loss of privacy and exposure of PII such as Social Security numbers) for which no adequate remedy at law exists.

316. Finally, all members of the proposed Classes are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

CAUSES OF ACTION

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

317. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

318. Excelsior required Plaintiffs and Class Members to submit non-public Private Information to it in order to obtain healthcare/medical services and/or employment.

319. By collecting and storing this data in its systems, and sharing it and using it for commercial gain, Excelsior had a duty of care to use reasonable means to secure and safeguard Plaintiffs' and Class Members Private Information, to prevent disclosure of the information, and to safeguard the information from theft. Excelsior's duty included a responsibility to implement processes by which it 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.

320. Excelsior's duties of care to Plaintiffs and Class Members include, but are not limited to:

a. exercising reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

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

c. having procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. employing reasonable security measures and otherwise protecting the Private Information of Plaintiffs and Class Members pursuant to HIPAA, the FTCA, industry standards, and New York General Business Law § 349;

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

f. promptly notifying Plaintiffs and Class Members of the Data Breach, and precisely disclosing the type(s) of information compromised.

321. Excelsior's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Excelsior and its employees, patients, and other affiliated persons, which is recognized by laws and regulations, including, but not limited to, HIPAA, as well as common law. Excelsior was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

322. Excelsior's duty to use reasonable security measures under HIPAA required it to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

323. In addition, Excelsior 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.

324. Excelsior'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 Excelsior is bound by industry standards to protect confidential Private Information.

325. Excelsior breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Excelsior 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 its 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; and

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

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

Breach was reasonably foreseeable given the known high frequency of cybersecurity attacks and data breaches in the healthcare industry.

327. 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.

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

329. Excelsior's negligent conduct is ongoing, in that, on information and belief, it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner. Plaintiffs and Class Members are also entitled to injunctive relief requiring Excelsior 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
(On Behalf of Plaintiffs and the Nationwide Class Against BCS)

330. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

331. BSC required Plaintiffs and Class Members to submit non-public Private Information to it in order to obtain healthcare/medical services and/or employment.

332. By collecting and storing this data in its systems, and sharing it and using it for commercial gain, BSC had a duty of care to use reasonable means to secure and safeguard Plaintiffs' and Class Members Private Information, to prevent disclosure of the information, and to safeguard the information from theft. BSC's duty included a responsibility to implement

processes by which it 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.

333. BSC's duties of care to Plaintiffs/Class Members include, but are not limited to:

a. exercising reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

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

c. having procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. employing reasonable security measures and otherwise protecting the Private Information of Plaintiffs and Class Members pursuant to HIPAA, the FTCA, industry standards, and New York General Business Law § 349;

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

f. promptly notifying Plaintiffs and Class Members of the Data Breach, and precisely disclosing the type(s) of information compromised.

334. BSC's duty of care to use reasonable security measures arose as a result of the special relationship that existed between BSC and its employees, patients, and other affiliated persons, which is recognized by laws and regulations, including, but not limited to, HIPAA, as well as common law. BSC was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

335. BSC's duty to use reasonable security measures under HIPAA required it to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure"

and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

336. In addition, BSC 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.

337. BSC'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 Excelsior is bound by industry standards to protect confidential Private Information. BSC breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by BSC 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 its networks and systems;
c. Failing to periodically ensure that its 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; and

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

338. It was foreseeable that BSC's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the Data Breach was reasonably foreseeable given the known high frequency of cybersecurity attacks and data breaches in the healthcare industry.

339. 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.

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

341. BSC's negligent conduct is ongoing, in that, on information and belief, it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

342. Plaintiffs and Class Members are also entitled to injunctive relief requiring BSC 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 III
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Nationwide Class Against Excelsior)

343. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

344. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Excelsior had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

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

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

347. Excelsior breached duties to Plaintiffs and Class Members under the Federal Trade Commission Act 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. Excelsior's failure to comply with applicable laws and regulations constitutes negligence per se.

349. But for Excelsior's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

350. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Excelsior's breach of its duties. Excelsior knew or should have known that it failed to meet its duties, and that its breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

COUNT IV
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Nationwide Class Against BSC)

352. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

353. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, BSC had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

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

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

356. BSC breached duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

357. BSC's failure to comply with applicable laws and regulations constitutes negligence per se.

358. But for BSC's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

359. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of BSC's breach of its duties. BSC knew or should have known that it failed to

meet its duties, and that its breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

COUNT V
BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class Against Excelsior)

361. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

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

363. Excelsior's Privacy Policy memorialized the rights and obligations of Excelsior 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.

364. In the Privacy Policy, Excelsior 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.

365. Plaintiffs and Class Members fully performed their obligations under their contracts with Excelsior.

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

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

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

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

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

371. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Excelsior 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 VI
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class Against Excelsior)

372. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

373. Plaintiffs and Class Members provided their Private Information to Excelsior in exchange for Excelsior's medical services, and they entered implied contracts with Excelsior pursuant to which Excelsior agreed to reasonably protect such information.

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

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

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

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

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

379. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Excelsior.

380. Excelsior breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information.

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

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

383. Plaintiffs and Class Members are also entitled to injunctive relief requiring Excelsior 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 long-term credit monitoring to all Class Members.

COUNT VII
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class Against BSC)

384. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

385. Plaintiffs and Class Members provided their Private Information to BSC in exchange for BSC's medical services, and they entered implied contracts with BSC pursuant to which BSC agreed to reasonably protect such information.

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

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

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

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

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

391. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with BSC.

392. BSC breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information.

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

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

395. Plaintiffs and Class Members are also entitled to injunctive relief requiring BSC 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 long-term credit monitoring to all Class Members.

COUNT VIII
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class Against Excelsior)

396. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

397. In light of the special relationship between Excelsior and Plaintiffs and Class Members, whereby Excelsior became guardian of Plaintiffs' and Class Members' Private Information, Excelsior became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members to: (1) safeguard Plaintiffs' and Class Members' Private Information; (2) timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) maintain complete and accurate records of what information (and where) Excelsior did and does store.

398. Excelsior has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationships with its current and former patients and employees to keep secure their Private Information.

399. Excelsior breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and provide detailed notice of the Data Breach to Plaintiffs and Class Members in a reasonable and practicable period of time.

400. Excelsior breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt, safeguard, and/or otherwise protect the integrity of Plaintiffs' and Class Members' Private Information.

401. Excelsior breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

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

403. As a direct and proximate result of Excelsior's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Excelsior's possession and is subject to further unauthorized disclosures so long as Excelsior fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Excelsior's services they received.

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

COUNT IX
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class Against BSC)

405. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

406. In light of the special relationship between BSC and Plaintiffs and Class Members, whereby BSC became guardian of Plaintiffs' and Class Members' Private Information, BSC became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members to: (1) safeguard Plaintiffs' and Class Members' Private Information; (2) timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) maintain complete and accurate records of what information (and where) BSC did and does store.

407. BSC has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationships with its current and former patients and employees to keep secure their Private Information.

408. BSC breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and provide detailed notice of the Data Breach to Plaintiffs and Class Members in a reasonable and practicable period of time.

409. BSC breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt, safeguard, and/or otherwise protect the integrity of Plaintiffs' and Class Members' Private Information.

410. BSC breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

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

412. As a direct and proximate result of BSC's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-

of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in BSC's possession and is subject to further unauthorized disclosures so long as BSC fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of BSC's services they received.

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

COUNT X
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class Against Excelsior)

414. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

415. Plaintiffs bring this claim individually and on behalf of all Class Members. This count is pleaded in the alternative to the breach of contract counts above.

416. Upon information and belief, Excelsior funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

417. As such, a portion of the payments made by or on behalf of Plaintiffs and the 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 Excelsior.

418. Plaintiffs and Class Members conferred a monetary benefit on Excelsior. Specifically, they purchased healthcare services or obtained employment from Excelsior and/or its agents and in so doing provided Excelsior with their Private Information. In exchange, Plaintiffs and Class Members should have received from Excelsior the healthcare services that were the subject of the transaction or employment they sought, and should have had their Private Information protected with adequate data security.

419. Excelsior knew that Plaintiffs and Class Members conferred a benefit which Excelsior accepted. Excelsior profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes. Without Plaintiffs' and Class Members' Private Information, Excelsior would be unable to provide healthcare services, staff its facilities, or charge patients for healthcare services.

420. In particular, Excelsior enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Excelsior instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and/or vendors. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Excelsior's decision to prioritize its own profits over the requisite security.

421. Under the principles of equity and good conscience, Excelsior should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Excelsior failed

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

422. Excelsior failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

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

424. If Plaintiffs and Class Members knew that Excelsior had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Excelsior.

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

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

and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

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

COUNT XI
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class Against BSC)

429. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

430. Plaintiffs bring this claim individually and on behalf of all Class Members. This count is pleaded in the alternative to the breach of contract counts above.

431. Upon information and belief, BSC funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

432. As such, a portion of the payments made by or on behalf of Plaintiffs and the 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 BSC.

433. Plaintiffs and Class Members conferred a monetary benefit on BSC. Specifically, they purchased healthcare services or obtained employment from BSC and/or its agents and in so doing provided BSC with their Private Information. In exchange, Plaintiffs and Class Members should have received from BSC the healthcare services that were the subject of the transaction or

employment they sought, and should have had their Private Information protected with adequate data security.

434. BSC knew that Plaintiffs and Class Members conferred a benefit which BSC accepted. BSC profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes. Without Plaintiffs' and Class Members' Private Information, BSC would be unable to provide healthcare services, staff its facilities, or charge patients for healthcare services.

435. In particular, BSC enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, BSC instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and/or vendors. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of BSC's decision to prioritize its own profits over the requisite security.

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

437. BSC failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

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

439. If Plaintiffs and Class Members knew that Excelsior had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to BSC.

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

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

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

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

COUNT XII
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class Against Excelsior)

444. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

445. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Excelsior and ultimately accessed and acquired in the Data Breach.

446. As a healthcare provider and employer, Excelsior has a special, fiduciary relationship with its patients and employees, including Plaintiffs and Class Members. Because of that special relationship, Excelsior was provided with and stored Plaintiffs' and Class Members' Private Information and had a duty to maintain such Information in confidence.

447. Patients like Plaintiffs and Class Members have a privacy interest in personal medical and other matters, and Excelsior had a duty not to disclose such matters concerning its patients.

448. As a result of the parties' relationship, Excelsior had possession and knowledge of highly sensitive and confidential Private Information belonging to Plaintiff and Class Members, information that was not generally known.

449. Plaintiffs and Class Members did not consent nor authorize Excelsior to release or disclose their Private Information to an unknown criminal actor.

450. Excelsior breached its duty of confidence owed to Plaintiffs and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Plaintiffs' and Class Members' Private

Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement adequate information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class Members' Private Information to a criminal third party.

451. But for Excelsior's wrongful breach of its duty of confidence owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

452. As a direct and proximate result of Excelsior's wrongful breach of its duty of confidence, Plaintiffs and Class Members have suffered and will continue to suffer the injuries alleged herein.

453. It would be inequitable for Excelsior to retain the benefit of controlling and maintaining Plaintiffs' and Class Members' Private Information at the expense of Plaintiffs and Class Members.

454. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT XIII
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class Against BSC)

455. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

456. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by BSC and ultimately accessed and acquired in the Data Breach.

457. As a healthcare provider and employer, BSC has a special, fiduciary relationship with its patients and employees, including Plaintiffs and Class Members. Because of that special relationship, BSC was provided with and stored Plaintiffs' and Class Members' Private Information and had a duty to maintain such Information in confidence.

458. Patients like Plaintiffs and Class Members have a privacy interest in personal medical and other matters, and BSC had a duty not to disclose such matters concerning its patients.

459. As a result of the parties' relationship, BSC had possession and knowledge of highly sensitive and confidential Private Information belonging to Plaintiff and Class Members, information that was not generally known.

460. Plaintiffs and Class Members did not consent nor authorize BSC to release or disclose their Private Information to an unknown criminal actor.

461. BSC breached its duty of confidence owed to Plaintiffs and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Plaintiffs' and Class Members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement adequate information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the

time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class members' Private Information to a criminal third party.

462. But for BSC's wrongful breach of its duty of confidence owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

463. As a direct and proximate result of BSC's wrongful breach of its duty of confidence, Plaintiffs and Class Members have suffered and will continue to suffer the injuries alleged herein.

464. It would be inequitable for BSC to retain the benefit of controlling and maintaining Plaintiffs' and Class Members' Private Information at the expense of Plaintiffs and Class Members.

465. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT XIV
VIOLATIONS OF THE NEW YORK DECEPTIVE ACTS AND PRACTICES ACT, N.Y. GEN. BUS. LAW § 349 ("GBL")
(On Behalf of Plaintiffs and the New York Class Against Excelsior)

466. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

467. This claim is brought on behalf of Plaintiffs and the New York Class against Excelsior.

468. Plaintiffs and Class Members are "persons" within the meaning of the N.Y. Gen. Bus. Law ("GBL") § 349(h).

469. Excelsior is a "person, firm, corporation or association or agent or employee thereof" within the meaning of GBL § 349(b).

470. Under GBL Section 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce" are unlawful.

471. Excelsior violated the GBL through its promises to protect, and subsequent failure to adequately safeguard and maintain, Plaintiffs' and New York Class Members' Private Information. Excelsior failed to notify Plaintiffs and other Class Members that, contrary to its representations about valuing data security and privacy, it does not maintain adequate controls to protect Private Information. Excelsior omitted all this information from Plaintiffs and New York Class Members.

472. As a result of Excelsior's above-described conduct, Plaintiffs and the New York Class have suffered damages from the disclosure of their information to unauthorized individuals.

473. The injury and harm that Plaintiffs and the New York Class suffered was the direct and proximate result of Excelsior's violations of the GBL. Plaintiffs and New York Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information, which remains in Excelsior's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) of overpayment for the services that were received without adequate data security.

474. Plaintiffs, individually and on behalf of the New York Class, request that this Court enter such orders or judgments as may be necessary to enjoin Excelsior from continuing its unfair and deceptive practices.

475. Under the GBL, Plaintiffs and New York Class Members are entitled to recover their actual damages or $50, whichever is greater. Additionally, because Excelsior acted willfully or knowingly, Plaintiffs and New York Class Members are entitled to recover three times their actual damages. Plaintiffs is also entitled to reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes set forth herein, respectfully pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Classes;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

E. Ordering Defendants to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: June 3, 2025

Respectfully submitted,

/s/ Jennifer Czeisler
Jennifer Cziesler
Arturo Pena*
Edward W. Ciolko*
STERLINGTON PLLC
One World Trade Center, 85th Floor
New York, NY 10007
Tel.: (929) 709-1493
jen.czeisler@sterlingtonlaw.com
arturo.pena@sterlingtonlaw.com
edward.ciolko@sterlingtonlaw.com

Deborah De Villa (NY Bar #5724315)
AHDOOT & WOLFSON, PC
521 5th Avenue, 17th Floor
New York, NY 10175
Tel: (917) 336-0171
Fax: (917) 336-0177
ddevilla@ahdootwolfson.com

Andrew W. Ferich**
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650

Radnor, PA 19087
Tel: (310) 474-9111
Fax: (310) 474-8585
aferich@ahdootwolfson.com

Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel: (212) 532-1091
tbean@sirillp.com

Interim Co-Lead Counsel for Plaintiffs and the Putative Class

** Admitted pro hac vice*

*** Pro hac vice application pending or to be filed*