UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MICHIGAN

SCOTT MANGOLD, individually and on behalf of all others similarly situated, Plaintiff, v. STRYKER CORPORATION, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Scott Mangold ("Plaintiff"), on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Stryker Corporation ("Stryker" or "Defendant"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII" or "Private Information")[1] and that was impacted in a data breach.

2. Defendant is "a global leader in medical technologies" and offers "innovative products and services in MedSurg, Neurotechnology and Orthopaedics."[2]

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

[2] Our Company, STRYKER, https://www.stryker.com/us/en/about.html (last visited March 19, 2026).

3. As such, Defendant stores a litany of highly sensitive PII about its current and former employees.

4. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard PII that was entrusted to them, and their accompanying responsibility to store and transfer that information.

5. Defendant lost control over Plaintiff's and Class Members' PII when cybercriminals infiltrated its insufficiently protected computer systems in a data breach.

6. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former employees' PII.

7. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII. In short, the Defendant's failures placed the Class's PII in a vulnerable position—rendering them easy targets for cybercriminals.

8. Indeed, the cybercriminal group "Handala" claimed responsibility for that attack and alleged to have targeted 200,000 critical systems of Striker, wiped approximately 12,000 terabytes of data, as well as gain access and exfiltrate files from Stryker's systems.[3]

9. Upon information and belief, Plaintiff' PII is available on the dark web as a result

[3] Michael Kan, *FBI Seizes Sites of Hacking Group Behind Data-Wiping Attack on Stryker*, PC MAG (Mar. 19, 2026), https://www.pcmag.com/news/fbi-seizes-sites-of-hacking-group-behind-data-wiping-attack-on-stryker

of the Data Breach.

10. As a result of the Data Breach, Plaintiff and Class Members, suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant's fail to undertake appropriate and adequate measures to protect the PII.

11. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and Class Members PII from a foreseeable and preventable cyber-attack.

12. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself, and all similarly situated individuals whose PII was accessed during the Data Breach.

13. The exposure of the PII to cybercriminals is a bell that cannot be unrung. Before this data breach, their PII was exactly that—private. Not anymore. Now, their PII is forever exposed and unsecure.

PARTIES

14. Plaintiff Scott Mangold is and was, at all times material hereto, a resident and citizen of Haddonfield, New Jersey where he intends to remain.

15. Defendant Stryker Corporation, is a for-profit corporation, incorporated in

Michigan and with its principal place of business at 1941 Stryker Way, Portage, Michigan 49002. Its registered agent, C T Corporations System, can be found at 40600 Ann Arbor Rd E Ste 201, Plymouth, Michigan 48170.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Members of the proposed Class are citizens of different states than Defendant, namely Plaintiff, a citizen of Colorado, and there are over 100 putative Class Members.

17. This Court has personal jurisdiction over Defendant because it is headquartered in Michigan, regularly conducts business, and has sufficient minimum contacts in Michigan.

18. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Background on Defendant

19. Stryker is "a global leader in medical technologies" that offers "innovative products and services in MedSurg, Neurotechnology and Orthopaedics"2 and made $22.6 billion in global sales in 2024.[4]

20. Stryker "impacts more than 150 million patients annually in 61 countries across the world"4 and has offices and manufacturing facilities in Michigan, California, Texas, Arizona,

[4] *Our Company*, STRYKER, https://www.stryker.com/us/en/about.html (last visited March 19, 2026).

Florida and New Jersey.[5]

21. As a part of their businesses Defendant collect and maintain the PII of thousands of its current and former employes.

22. Plaintiff and Class Members are comprised of current and former employees of Defendant. The PII provided by Plaintiff and Class Members includes, but is not limited to names, contact information, dates of birth, social security numbers, driver's licenses, financial account information.

23. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with their internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.[6]

24. Further, Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

25. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, and to make only authorized disclosures of this information.

26. As a result of collecting and storing the PII of Plaintiff and Class Members for their own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' PII from disclosure to third parties.

---

[5] *2024 Comprehensive Report*, STRYKER, https://www.stryker.com/content/dam/stryker/about/annual-review/2024/Stryker-2024-Comprehensive-Report.pdf (last visited March 19, 2026).

[6] *See Privacy Statement*, STRYKER, https://www.stryker.com/us/en/legal/privacy.html (last visited March 19, 2026).

27. On information and belief, Defendant has not implemented reasonably cybersecurity safeguards or policies to protect Plaintiff's and Class Members' PII or supervised its providers and employees to prevent, detect, and stop breaches of their network or systems. As a result, Defendant leaves significant vulnerabilities in their systems for cybercriminals to exploit and gain access to Plaintiff's and Class Members' PII.

The Data Breach

28. On or around March 11, 2026, Defendant was subject to a criminal cyberattack that impacted their system (the "Data Breach").[7]

29. Upon information and belief, the cybercriminal group Handala exfiltrated approximately 50 terabytes of critical data was exfiltrated from Stryker's network and systems, including the PII of Plaintiff and the Class Members.[8] Below is a screenshot of Handala's Dark Web website post claiming responsibility for the attack.

[7] Stryker Corporation Form, Current Report (Form 8-K) (Mar. 11, 2026).
[8] Eduard Kovacs, *Iranian Hackers Likely used malware-Stolen Credentials in Stryker Breach*, SECURITY WEEK (Mar. 18, 2026), https://www.securityweek.com/iranian-hackers-likely-used-malware-stolen-credentials-in-stryker-breach/.

Stryker Corporation Hacked

2026-03-11

We announce to the world that, in retaliation for the brutal attack on the Minab school and in response to ongoing cyber assaults against the infrastructure of the Axis of Resistance, our major cyber operation has been executed with complete success.

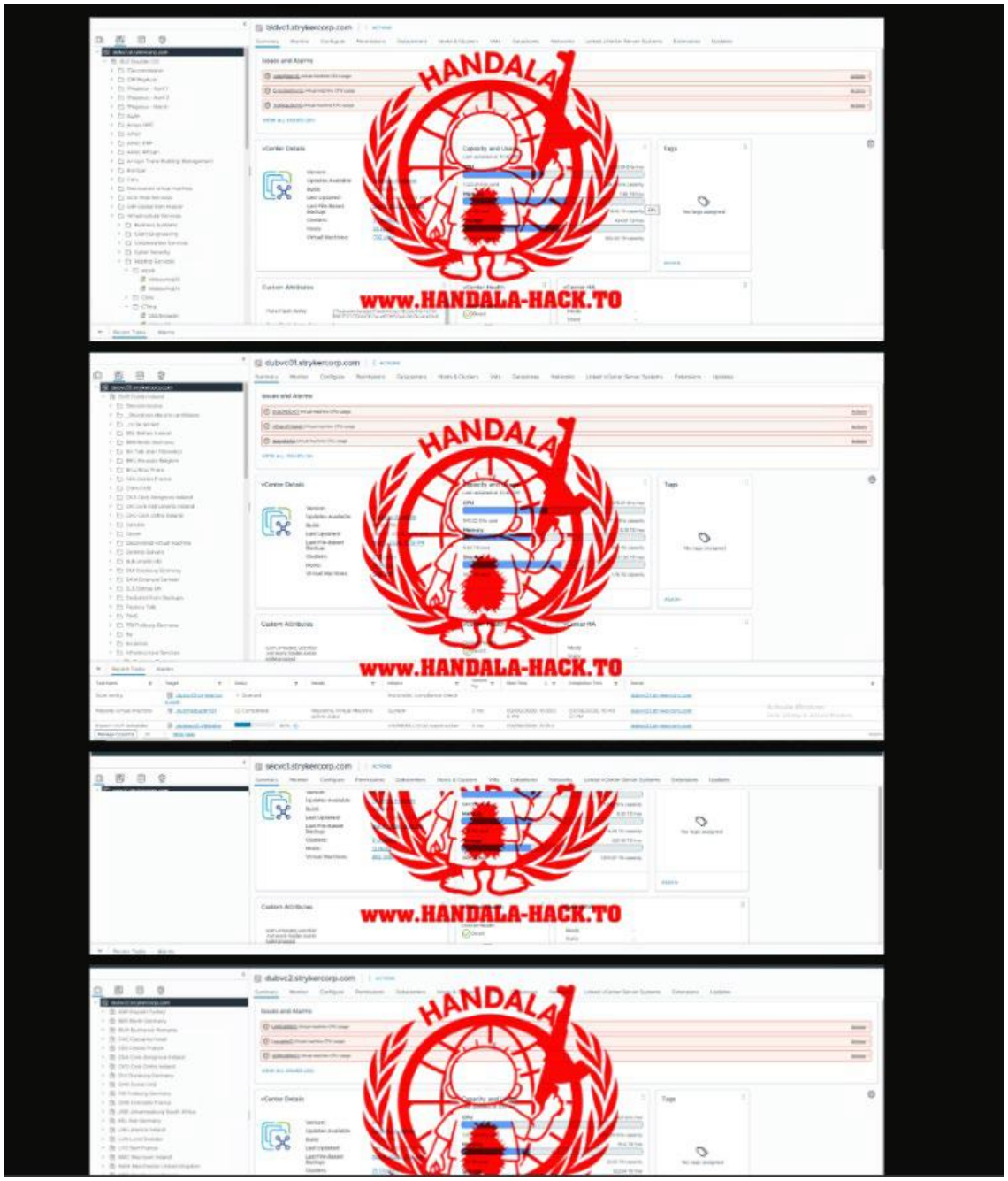
The Zionist-rooted corporation, Stryker, one of the key arms of the global Zionist lobby and a central ring in the 'New Epstein' chain, has been struck with an unprecedented blow. In this operation, over 200,000 systems, servers, and mobile devices have been wiped and 50 terabytes of critical data have been extracted.

Stryker's offices in 79 countries have been forced to shut down. All the acquired data is now in the hands of the free people of the world, ready to be used for the true advancement of humanity and the exposure of injustice and corruption.

A clear warning to all Zionist leaders and their lobbies who hide behind concrete walls and closed windows:
The era of the 'Epstein' rings and the demons of our time is over. 'Nimrod of this era,' even if you close your windows, we will build our nests everywhere. Get ready for the mosquito...

This is only the beginning of a new chapter in cyber warfare. To all those plotting attacks on the infrastructure of the Axis of Resistance:
The era of hit-and-run is over!

30. Moreover, Handala's posted a sample of the documents exfiltrated from Strkyers system.[9] An example of such can be seen below:



[9] Mike Clair, *Stryker Cyberattack Update: Iran-Linked Handala Group Claims Destructive Wiper Attack on Medical Tech Giant*, INTERNATIONAL BUSINESS TIMES (Mar. 12, 2026) https://www.ibtimes.com/stryker-cyberattack-update-iran-linked-handala-group-claims-destructive-wiper-attack-medical-tech-3799024

31. Defendant already admitted that the Data Breach affected "certain information technology systems . . . that has resulted in a global disruption to the [Stryker's] Microsoft environment." The Data Breach "has caused, and is expected to continue to cause, disruptions and limitations of access to certain of [Stryker's] information systems and business applications supporting aspects of [Stryker's] operations and corporate functions."[10]

32. The number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control. And upon information and belief, the putative class is over one hundred members—as it includes its current and former employees.

33. Defendant has not begun notifying impacted individuals about the Data Breach, and instead provided vague updates on its website to customers.[11]

34. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

35. Indeed, the only details Defendant has provided regarding the Data Breach itself is that the attack was not a "ransomware" attack, and that they have not found evidence of malware deployed to their systems.[12]

---

[10] Stryker Corporation Form, Current Report (Form 8-K) (Mar. 11, 2026).
[11] *Customer Updates: Stryker Network Disruption*, STRKER (MAR. 15, 2026), https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html.
[12] *Id.*

36. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including (a) that this Data Breach was the work of cybercriminals; (b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and (c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiff's and Class Members' PII.

37. Defendant lost control over that data when cybercriminals infiltrated and Defendant insufficiently protected computer systems in the Data Breach, resulting in cybercriminals having unfettered access and, upon information and belief, the exfiltration of Plaintiff's and Class Members' PII.

38. Upon information and belief, the cybercriminals were able to infiltrate Defendant's information systems for an extended period of time.[13]

39. Given that the hackers were able to infiltrate Defendant's information systems for an extended period of time and perform malicious activity—including reconnaissance and data exfiltration functions that should have had alarm bells ringing—it is likely that Defendant failed to implement reasonable industry standard cybersecurity safeguards sufficient to detect malicious activity in a timely manner, including monitoring, logging, and alerting systems such as EDR, XDR, data loss prevention tools, and centralized alerting and logging.

40. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to Plaintiff

[13] Eduard Kovacs, *Iranian Hackers Likely used malware-Stolen Credentials in Stryker Breach*, SECURITY WEEK (Mar. 18, 2026), https://www.securityweek.com/iranian-hackers-likely-used-malware-stolen-credentials-in-stryker-breach/.

and Class Members' PII.

41. Indeed, it appears that Defendant filed to perform elementary function such as resetting credentials for administrative accounts on a regular basis.

42. SecurityWeek reported that "[a]n analysis of infostealer malware logs, which contain information stolen by such malware, revealed that credentials for Stryker administrator accounts were harvested, alongside dozens of other Microsoft service credentials and mobile device management (MDM) credentials associated with the medtech company. . . . 'Most of these creds are months if not years old, which would have given Stryker more than enough time to reset and avoid a breach.'"[14]

43. Given the Defendant's failure in even the most basic requirements of cybersecurity, it is likely that Defendant's cybersecurity program as a whole is severely inadequate in comparison to the measures it is legally obligated to provide to individuals for whom it collects Personal Information, thus leaving them exposed to the Data Breach that indeed came into fruition.

44. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damage they have suffered because of the Data Breach. Even if Defendant eventually offers several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.[15]

45. Because of the Data Breach, the sensitive PII of Plaintiff and Class Members was

---

[14] *Id.* (quoting Alon Gal, CTO of threat intelligence firm Hudson Rock).

[15] Chi Chi Wu, *Essentials About Credit reporting: Consumer Debt Advice form NCLC*, NAT'L CONSUMER L. CTR. (July 6, 2018), https://library.nclc.org/article/essentials-about-credit-reporting-consumer-debt-advice-nclc (explaining how most negative information stays on your credit report for seven years).

placed into the hands of cyber criminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

46. Defendant owed a duty to protect Plaintiff and Class Members from the harm of the Data Breach.

47. Defendant owed a duty to protect Plaintiff and Class Members from the harm that insufficient data security and the consequential exposure of PII would cause because such harm was foreseeable and reasonably preventable.

48. Defendant knew of the ubiquity of data breaches in the industry and that any breach of its network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the tens of thousands individuals whose PII was compromised, as well as intrusion into their private and sensitive financial matters.

49. Defendant failed to implement and adequate and reasonable means to meet the industry, and FTC standards, as well as failed to protect its employees.

50. The Data Breach is the direct result of Defendant's failure to implement basic data security measures over Plaintiff's and Class Members' data in its custody and control. Had Defendant implemented reasonable cybersecurity measures—including adequate safeguards for initial access, encryption, or redaction of personal data elements, and sufficient logging, monitoring, and alerting tools to detect unauthorized activity—cybercriminals would not have been able to hack into Defendant's network, perform reconnaissance necessary to locate Plaintiff's and Class Members' PII, and then exfiltrate that data before being detected.

51. Defendant's tortious conduct and breach of contractual obligations, as detailed in herein, are evidence by its failure to identify the scope of information involved and/or individuals impacted by the Data Breach until months after cybercriminals breached its network and accessed

Plaintiff's and Class Members' Private stored therein—meaning Defendant had no effective means in place to ensure that cyberattacks were detected, prevented, or timely investigated.

52. As a result of the Data Breach, Plaintiff and Class Members now face an increased risk of fraud and identity theft, among many other actual and imminent damages.

53. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches.

54. Because of the Data Breach, the sensitive PII of Plaintiff and Class Members was placed into the hands of cyber criminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

The Data Breach Was a Foreseeable Risk of Which Defendant Was on Notice

55. Plaintiff and Class Members value their PII, as in today's electronic-centric world, their PII is required for numerous activities, such as verifying eligibility for employment, opening a new bank account or securing access to credit at favorable rates, and accessing benefits.

56. In light of recent high profile data breaches, Defendant knew or should have known that its electronic records would be targeted by cybercriminal.

57. In 2024, there were 3,158 data breaches with 1,350,835,988 victim notices, a 211% increase year over year.[16]

58. In April 2020, ZDNet reported, in an article tilted "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate

[16] 2024 DATA BREACH REPORT 6, IDENTITY THEFT RES. CTR. (Jan. 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf.

negative news for companies as revenge against those who refuse to pay."[17]

59. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion." [18]

60. Defendant's data security obligations were also particularly important given the substantial increase in Data Breaches in the healthcare industry preceding the date of the breach. Because of the value of its collected and stored data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

61. Indeed, "Comparitech disclosed that in the first nine months of 2025, 293 ransomware attacks were recorded on hospitals, clinics, and other direct care providers. An additional 130 attacks targeted business within the healthcare sector, including pharmaceutical manufactures, medical billing providers, and healthcare tech companies."[19]

62. The healthcare industry consistently reports as the industry with the highest, or one of the highest, number of data breaches.[20]

---

[17] Catalin Cimpanu, *Ransomware Mentioned in 1,000+ SEC Filings Over the Past Year*, ZDNET (April 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/.

[18] *Stop Ransomware Guide*, CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last visited Mar. 19, 2026).

[19] Anna Riberio, *Healthcare Ransomware Attacks Surge 30% in 2025, as Cybercriminals Shift Focus to Vendors and Service Partners*, COMPARITECH (Oct. 13, 2025), https://industrialcyber.co/reports/healthcare-ransomware-attacks-surge-30-in-2025-as-cybercriminals-shift-focus-to-vendors-and-service-partners/.

[20] IDENTITY THEFT RES. CTR., 2024 DATA BREACH REPORT 6, IDENTITY THEFT RES. CTR. 25 (Jan. 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf.

63. Further, "[i]n 2024, the healthcare industry experienced a concerning surge in data breaches, with over 300 million patient records compromised—a 26% increase from 2023."[21]

64. 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."[22]

65. 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."[23]

66. The HIPAA Journal article goes on to explain that records, are "often processed and packaged with other illegally obtained data to create full record sets (known as "Fullz" package) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites 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."[24]

67. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to

---

[21] BLUESENSE, BREACH BAROMETER ANNUAL REPORT 2 (2025), https://bluesight.com/wp-content/uploads/2025/02/2025-Breach-Barometer-Annual-Report.pdf.
[22] *5 Important Elements to Establish Data Security in Healthcare*, ADVENT HEALTH UNIV. (May 21, 2020), https://www.ahu.edu/blog/data-security-in-healthcare.
[23] *Id.*
[24] *Id.*

potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

68. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in 2020.[25]

69. These significant increases in attacks to companies, particularly those in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant.

70. This readily available and accessible information confirms that, prior to the Data breach, Defendant knew or should have known that (i) cybercriminals were targeting entities such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of entities such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) the cybercriminal tactics included threatening to release stolen data.

71. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as a result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

72. Defendant knew or should have known that it should have encrypted its employees' PII to protect against their publication and misuse in the event of a cyberattack.

Defendant Could Have Prevented the Data Breach

73. Data breaches are preventable.[26] Indeed, the American Bar Association published a treatise titled the Data Breach and Encryption Handbook wherein the author explained that:

---

[25] Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SEC. MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.
[26] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH & ENCRYPTION HANDBOOK (2012).

a. "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." [27]

b. "Organizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[28]

c. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."[29]

Defendant Fails to Comply with FTC Guidelines

74. 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.

75. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer 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

[27] *Id.* at 17.
[28] *Id.* at 28.
[29] *Id.*

security problems.[30]

76. 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.

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

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

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

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

data security obligations.

80. Defendant failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

81. Defendant at all times fully aware of its obligation to protect the PII of employees. Defendant was also aware of the significant repercussions that would result from their failure to do so.

Defendant Failed to Comply with Industry Standards

82. As shown above, experts studying cyber security routinely identify businesses such as the Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with at least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

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

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[31]

84. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . . .

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the Internet for the sender organization's website or

[31] HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE 3–4, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (U.S. Government Interagency technical guidance document) (last visited Mar. 19, 2026).

> the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . . .
>
> - **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
>
> - **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it . . . .
>
> - **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
>
> - **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> - **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . . .[32]

85. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure Internet-facing assets**
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
> - Prioritize and treat commodity malware infections as potential full compromise;
>
> **Include IT Pros in security discussions**

---

[32] *Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (April 11, 2019), https://www.cisa.gov/news-events/news/protecting-against-ransomware (revised Sept. 2, 2021).

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[33]

86. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

87. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation 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 all established standards in reasonable cybersecurity readiness.

88. The foregoing frameworks are existing and applicable industry standards in the

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

healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

The Data Breach Caused Plaintiff and the Class Members Injury and Damages

89. Plaintiff and members of the proposed Class have suffered injury and damages from the unauthorized disclosure and misuse of their PII disclosed in the Data Breach that can be directly traced to Defendant, that has occurred, is ongoing, and/or will imminently occur.

90. Data Breaches such as the one experienced by Plaintiff and Class Members are especially problematic because of the disruption they cause to the daily lives of victims affected by the attack.

91. As stated prior, on information and belief, in the Data Breach, cybercriminals were able to access the Plaintiff's and the proposed Class Members' PII, which is now being used or will imminently be used for fraudulent purposes and/or has been sold for such purposes and posted on the Dark Web for sale, causing widespread injury and damages.

92. Once an individual's PII is for sale and access on the dark web, cybercriminals are able to use the stolen and compromised to gather and steal even more information. [34]

93. The ramifications of Defendant's failure to keep Plaintiff's and the Class Members' PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, medical information or other information, such as addresses, without permission, to commit fraud or other crimes.

94. Because Defendant failed to prevent the Data Breach, Plaintiff and the proposed

---

[34] Ryan Toohil, *What do Hackers do with Stolen Information*, AURA, (September 5, 2023) https://www.aura.com/learn/what-do-hackers-do-with-stolen-information.

Class Members have suffered, will imminently suffer, and will continue to suffer injury-in-fact and damages, including but not limited to:

a. The loss of the opportunity to control how PII is used;

b. Unauthorized use of stolen PII;

c. Dramatic increase in spam telephone calls;

d. Emotional distress;

e. The compromise and continuing publication of their PII;

f. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud, and for necessary credit monitoring and identity theft protection;

g. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying 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 and fraud;

h. The diminution in value of their PII; and,

i. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fail to undertake the appropriate measures to protect the PII in its possession.

The Data Breach Caused Plaintiff and the Class Increased Risk of Identity Theft

95. The Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

96. Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because Defendant's failures resulted in Plaintiff's and Class Members' PII falling into the hands of identity thieves.

97. The unencrypted PII of Class Members has already or will end up for sale on the dark web, because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the PII for the express purpose of conducting financial fraud and

identity theft operations.

98. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[35] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[36] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[37]

99. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

100. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information…[is] worth more than 10x on the black market."[38]

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

102. Because a person's identity is akin to a puzzle with multiple data points, the more

---

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

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

[37] *For Sale in the Dark*, VPNOverview, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark (last visited mar. 19, 2026).

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

accurate pieces of data an identity thief obtains about a person, the easier it is for the cybercriminal to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

103. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

104. Further, the standard operating procedure for cybercriminals is to use some data, like the PII here, to access "Fullz packages" of that person to gain access to the full suite of additional PII that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victims' information to perpetrate even more types of attacks.

105. With "Fullz" packages, cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

106. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it

at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

107. Further, using this technique, identity thieves piece together full pictures of victims' information to perpetrate even more types of attacks.

108. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.

109. Additionally, Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[39] (Emphasis added).

110. 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

---

[39] *Dark Web Monitoring: What You Should Know*, CONSUMER FED'N OF AM. (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[40]

111. Individuals, like Plaintiff and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hackers' purposes.

112. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other PII increases."[41] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[42]

113. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items

---

[40] *Identity Theft and Your Social Security Number*, SOC. SEC. ADMIN. 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[41] *See Avoid Identity Theft*, SOC. SEC. ADMIN., https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases (last visited Mar. 19, 2026).
[42] *Id.*

you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[43]

114. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[44] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[45]

115. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[46]

116. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[47]

117. According to the national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number,

---

[43] *Identity Theft and Your Social Security Number*, SOC. SEC. ADMIN. (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[44] *See How to Protect Yourself from Social Security Number Identity Theft*, EQUIFAX, https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited Mar. 19, 2026).
[45] *See* Julia Kagan, *What Is a SSN? What to Know About Social Security Numbers*, INVESTOPEDIA (Sept. 2, 2024) https://www.investopedia.com/terms/s/ssn.asp.
[46] Anna Tong, *Hackers Stole Consumers' License Numbers from Geico in Months-Long Breach*, FORBES (Apr. 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-consumers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658.
[47] *Id.*

> your driver's license number is one of the most important pieces of information to keep safe from thieves.

118. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[48] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[49]

119. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[50]

120. 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 unemployment benefits, or apply for a job using a false identity. 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.

121. Data Breach victims suffer long-term consequences when their social security numbers are taken and used by hackers. Even if they know their social security numbers are being

---

[48] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO MAG. (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/.

[49] *Id.*

[50] *How Identity Thieves Took My Wife for a Ride,* NY Times (April 27, 2021), https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html.

misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

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

123. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[51]

124. Similarly, 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 PII, such as your name and address, remains the same."[52]

---

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

[52] *Identity Theft and Your Social Security Number*, Pub. No. 05-10064, SOCIAL SEC. ADMIN. (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

125. Further, the California state government states that "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[53]

126. The FTC recommends that identity theft victims take several costly steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.[54]

127. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls. For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Moreover, thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated.[55]

128. What's more, theft of PII is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected

---

[53] *See Your Social Security Number: Controlling the Key to Identity Theft*, CAL. DEPT. JUST. https://oag.ca.gov/idtheft/facts/your-ssn (last visited Mar. 19, 2026).
[54] *What To Do Right Away*, FTC (2024), https://www.identitytheft.gov/Steps.
[55] *The Identity Theft Resource Center's 2021 Consumer Aftermath Report Reveals Impacts on Covid-19 Identit Crime Victims*, IDENTITY THEFT RES. CTR. (May, 26, 2021), https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/.

through the lens of massively complex cloud computing, PII are valuable property rights.

129. PII 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.

130. Where the most PII belonging to Plaintiff and Class Members was accessible from Defendant's network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

131. Further, there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied 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.[56]

132. Thus, Plaintiff and the Class Members must vigilantly monitor their financial and credit accounts for many years to come.

133. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein.

---

[56] *See* GAO Report, at p. 29.

134. Defendant knew or should have known of these harms which would be caused by the Data Breach they permitted to occur and strengthened its data systems accordingly.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

135. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and Defendant arguing that the individual failed to mitigate damages.

136. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff's and Class Members' Social Security numbers or other government identification are affected.

137. By spending this time, Plaintiff was not manufacturing his own harm, he was taking necessary steps at Defendant's direction and because the Data Breach included their Social Security numbers.

138. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

139. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims

of identity theft will face "substantial costs and time to repair the damage to her good name and credit record."[57]

Diminution in Value of Private Information

140. PII is a valuable property right.[58] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

141. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[59]

142. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[60]

143. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[61]

144. Conversely, sensitive PII can sell for as much as $363 per record on the dark web

---

[57] *See* GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T OFFICE, (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[58] *See, e.g.*, Randall 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) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[59] David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, L.A. TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[60] *See e.g.*, https://datacoup.com/ (last visited Mar. 19, 2026).

[61] *Frequently Asked Questions*, NIELSON COMPUT. & MOBIL PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Mar. 19, 2026).

according to the Infosec Institute.[62]

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

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

146. Based on the value of the information stolen, the data either has or will be sold to cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

147. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

148. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

---

[62] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

Lost Benefit of the Bargain

149. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide Defendant with their PII under certain terms, Plaintiff and Class Members understood and expected that Defendant would properly safeguard and protect their PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members employment of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Experience and Injuries

150. Plaintiff is a former employee of Defendant. In order to receive employment from Defendant, Defendant required Plaintiff to provide his PII.

151. Upon information and belief, at the time of the Data Breach, Defendant maintained Plaintiff's PII in its system.

152. Plaintiff is very careful about sharing his PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's grossly inadequate data security policies.

153. In order to obtain employment from Defendant, Plaintiff was required to provide his PII to Defendant, including among other things, his name, date of birth, contact information, Social Security number, driver's license number, and financial account information.

154. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff 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.

155. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors his PII multiple times a week and has already spent valuable time Plaintiff otherwise would have spent on other activities.

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

157. Upon information and belief, as a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

158. Indeed, around the time of the Data Breach, Plaintiff received a Dark Web alert from LifeLock alerting him that his PII, including an email and password he used during his time he worked with Stryker, was found on the Dark Web.

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

160. As a result of the Data Breach and given Defendant's explicit instructions, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

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

162. Plaintiff has a continuing interest in ensuring his PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

163. Plaintiff greatly values his privacy, and would not have provided his PII, undertaken the services and paid the amounts that he did if he had known that his PII would be maintained using inadequate data security systems.

CLASS ALLEGATIONS

164. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by Stryker Corporation in March 2026.

165. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

166. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

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

168. Numerosity: The Class is so numerous that joinder of all Members is impracticable. The identity of these individuals are within the exclusive knowledge of and can be ascertained only by resort to Defendant's records. Defendant has the administrative capability through its computer systems and other records to identify all Class Members, and such specific information is not otherwise available to Plaintiff.

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

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

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

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

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

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

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

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

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

j. Whether Defendant was unjustly enriched;

k. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

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

170. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

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

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

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

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

a. The unnamed Class Members are unlikely to have an interest in individually controlling the prosecution of separate actions;

b. Concentrating the litigation of the claims in one forum is desirable; Plaintiff anticipate no difficulty in the management of this litigation as a class action; and

c. Plaintiff's legal counsel has the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

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

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

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

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

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

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

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

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

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

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

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

180. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to current and former student names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing constitutionally sufficient notice

CAUSES OF ACTION

COUNT I
Negligence and Negligence *Per Se*
(On Behalf of Plaintiff and the Class against Defendant)

181. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

182. Plaintiff brings this claim individually and on behalf of the Class Members.

183. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

184. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

185. Defendant had, and continue to have, a duty to timely disclose that Plaintiff's and Class Members' PII within its possession was compromised and precisely the types of information that were compromised.

186. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected individuals' PII.

187. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff's and Class Members' PII. Various FTC publications and orders also form the basis of Defendant's duties.

188. In particular, Defendant has duty of care to use reasonable security measures arose as a result of a special relationship that existed between it and its employees. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

189. By accepting, collecting, and storing employees' PII, Defendant took on the obligation and duty to safeguard the highly sensitive PII from unauthorized disclosures, but failed to do so.

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

191. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII.

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

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems and to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee information; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

d. Failing to detect the breach at the time it began or within a reasonable time thereafter; and

e. Failing to follow their own privacy policies and practices published to their employees.

193. Defendant's conduct went far beyond ordinary negligence. Defendant acted with consciously and recklessly disregarded known risks to Plaintiff's PII, including by failing to implement basic and industry-standard cybersecurity measures, failing to adequately monitor its systems for unauthorized access, failing to remediate known security vulnerabilities, failing to properly train employees on data security, and failing to timely detect and prevent the Data Breach. Defendant knew or should have known that their inadequate data-security practices created a high

probability of harm to Plaintiff and the Class, yet Defendant consciously failed to take reasonable steps to prevent that harm.

194. Defendant's negligent conduct demonstrated a substantial lack of concern for whether injury would result to Plaintiff and the Class. Defendant's actions and omissions constituted a reckless indifference to the rights, safety, and interests of Plaintiff and the Class, whose sensitive personal and medical information Defendant was entrusted to protect.

195. Further, Defendant acted negligently by ignoring its duty to protect Plaintiff's PII, despite the ubiquity of data breaches in the healthcare industry as described above. Defendant's actions and omissions constituted a reckless indifference to the rights, safety, and interests of Plaintiff and the Class, whose sensitive personal information Defendant was entrusted to protect.

196. Moreover, Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and by failing to comply with industry standards.

197. Defendant' conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

198. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

199. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

200. Defendant, through its actions and/or omissions, unlawfully breached its duties to

Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Defendant's possession.

201. Defendant, through its actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

202. Defendant, through its actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

203. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' PII. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the PII they keep; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

204. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

205. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in injuries to Plaintiff and Class Members.

206. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

207. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

208. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their PII had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

209. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class against Defendant)

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

211. Defendant required Plaintiff and Class Members to provide and entrust their PII to Defendant as a condition of obtaining employment from Defendant.

212. Plaintiff and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect their PII and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

213. Defendant entered into implied contracts with Plaintiff and Class Members by collecting their PII and promising to safeguard it against unauthorized disclosures. Defendant entered into implied contracts with Plaintiff and Class members by accepting, collecting, storing, and maintaining the PII given to it by Defendant in exchange for safeguarding the PII from unauthorized disclosures. Defendant breached the implied contracts with Plaintiff and Class Members by failing to protect their PII from cybercriminals.

214. Defendant promised and warranted to Plaintiff and Class Members, to maintain the privacy and confidentiality of the PII Defendant collected from Plaintiff and Class Members and to keep such information safeguarded against unauthorized access and disclosure.

215. Defendant's adequate protection of Plaintiff's and Class Members' PII was a material aspect of these implied contracts.

216. Plaintiff and Class Members conferred a monetary benefit on Defendant in that Plaintiff and Class Members were required to provide the PII, perform services for Defendant, and generated revenue for Defendant, a portion of which should have been specifically allocated towards adequate data security.

217. Defendant accepted possession of Plaintiff's and Class Members' PII for the purpose of providing goods and services and implicitly agreed to protect their PII from data breaches and keep it confidential and secured.

218. The implied promise included consideration beyond those pre-existing general duties owed under state and federal regulations. The additional consideration included implied

promises to take adequate steps to comply with specific industry data security standards and FTC guidelines and industry standards on data security.

219. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII also protect the confidentiality of that data; (2) taking steps to ensure that the PII that is placed in the control of their agents is restricted and limited to achieve an authorized (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the PII against data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

220. Based on this implicit understanding, Plaintiff and Class Members accepted Defendant's offers and provided Defendant with their PII to obtain good and services and employment.

221. Plaintiff and Class Members would not have permitted their PII to be collected and stored by Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

222. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

223. Defendant materially breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII, by failing to adhere to FTC guidelines and industry standards, or by ensuring that their provider had adequate safeguards to protect the PII, and by failing to provide Plaintiff and Class Members with timely and accurate notice of the Data Breach.

224. As a result of Defendant's failures to fulfill the data security protections promised, Plaintiff and Class Members did not receive the full benefit of their bargains with Defendant, and

instead received services of a diminished value compared to that described in the implied contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

225. As a direct and proximate result of Defendant's breach of their implied contracts with Plaintiff and Class Members and the consequential Data Breach, Plaintiff and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

226. Upon information and belief, Defendant has not provided Plaintiff and the Class with information regarding the root cause of the Data Breach and the steps Defendant is taking to ensure that the PII remains safe and protected from further disclosures.

227. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of their implied contracts with Plaintiff and Class Members.

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

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class against Defendant)

229. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

230. Upon information and belief, Defendant fund their data security measures entirely from their general revenues, including from revenue generated by its employees, including Plaintiff and Class members, for which Defendant collected and maintained Plaintiff's and Class Members' PII.

231. As such, Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII and their employment services a portion of value and monies derived from Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each made that is allocated to data security is known to Defendant.

232. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

233. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

234. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

235. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

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

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

238. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft;

(ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) 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; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

240. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds they unjustly received from them.

FOURTH CAUSE OF ACTION
Invasion of Privacy—Intrusion Upon Seclusion and Public Disclosure of Private Facts
(On Behalf of Plaintiff and the Class against Defendant)

241. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

242. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

243. Plaintiff and Class Members successfully took reasonable and appropriate steps to

keep their PII confidential from the public.

244. Defendant owed a duty to its employees, including Plaintiff and the Class, to keep this information confidential.

245. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

246. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant in order to receive services, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

247. Defendant's conduct also represents a public disclosure of private facts in that the disclosure was made to cybercriminals—individuals in a special relationship with Plaintiff and the proposed Class in that they are the exact group from whom the expected cybersecurity measures are intended to protect Plaintiff and the proposed Class.

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

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

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

251. By intentionally failing to keep Plaintiff's and Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff' and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

252. As the Restatement explains, as used throughout the Restatement of Torts, intent "has reference to the consequences of an act rather than the act itself." Restatement (Second) of Torts § 8A, cmt. A (1964). "Intent is not, however, limited to consequences which are desired. If the actor knows that the consequences are certain, or substantially certain, to result from her act, and still goes ahead, she is treated by the law as if she had in fact desired to produce the result." *Id.* cmt. B.

253. Indeed, given the foreseeability of the harms inherent in data breaches and the ubiquitous nature of data breaches, Defendant was substantially certain that its failure to implement reasonable cybersecurity standards would lead to an invasion of Plaintiff's privacy.

254. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

255. As a proximate result of Defendant's acts and omissions, the PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

256. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class

because their PII is still maintained by Defendant with its inadequate cybersecurity system and policies.

257. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

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

PRAYER FOR RELIEF

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

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and his counsel as Class Counsel;

(b) For an order declaring that Defendant's conduct violates the laws referenced herein;

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

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

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

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

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

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: March 19, 2026

/s/ David H. Fink
David H. Fink (P28235)
Nathan J. Fink (P75185)
FINK BRESSACK
Bloomfield Hills, MIC 48304
Telephone: (248) 971-2500
dfink@finkbressack.com
nfink@finkbressack.com

J. Gerard Stranch, IV*
Grayson Wells*
Samuel Douthit*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Ave., Ste. 200
Nashville, TN 37203
(615) 254-8801
(615) 255-5419
gstranch@stranchlaw.com
gwells@stranchlaw.com
sdouthit@stranchlaw.com

Attorneys for Plaintiff and the Proposed Class

* Application for admission to be submitted