ZIMMERMAN REED LLP
Caleb Marker (SBN 269721)
E-mail: caleb.marker@zimmreed.com
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780 Telephone
(877) 500-8781 Facsimile

GIBSON CONSUMER LAW GROUP, LLC
MaryBeth V. Gibson
E-mail: marybeth@gibsonconsumerlawgroup.com
4279 Roswell Road
Suite 208-108
Atlanta, GA 30342
(678) 642-2503 Telephone

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

HEIDI HUMPHREYS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

AMGEN INC.,

Defendant.

CASE NO.: 2:26-cv-08688

COMPLAINT
ACTION SEEKING STATEWIDE OR NATIONWIDE RELIEF

1. Negligence
2. Negligence *per se*

(Plaintiff Demands Trial by Jury)

Plaintiff Heidi Humphreys ("Plaintiff"), by and through her undersigned counsel, file this Class Action Complaint individually and on behalf of a class of all similarly situated persons against Defendant Amgen Inc. ("Amgen" or "Defendant"). Plaintiff alleges the following based upon personal knowledge, information and belief, and the investigation of counsel.

I. NATURE OF THE ACTION

1. Defendant is a multinational biotechnology company that develops, manufactures, and commercializes prescription medicines for the treatment of cancer, cardiovascular disease, inflammation, rare diseases, and other serious medical conditions.

2. In that capacity, Amgen has directly and indirectly collected highly sensitive personally identifiable information ("PII") such as names, addresses, contact information, financial and billing information, and employment information, and protected health information ("PHI") such as health insurance information, health conditions, diagnoses, medical appointment and test information, prescription information, and payment and billing information (collectively "Sensitive Private Information") from thousands of patients and customers. Plaintiffs and Class Members were required to entrust Defendant with a vast array of such Sensitive Private Information.

3. Taking reasonable, standard precautions against cybercrime and data breaches is a fundamental part of doing business in the modern age—especially for businesses in the healthcare sector that routinely collect and store highly confidential information like the Sensitive Private Information at issue here.

4. By collecting and maintaining Plaintiff's and the Class Members' Sensitive Private Information, Defendant was required by law to exercise reasonable care and comply with industry and statutory requirements to protect that information. Indeed, Amgen acknowledges:

> The lawful collection and use of such information is important to Amgen's business activities. U.S. federal and state laws and the laws of other countries require companies to implement certain safeguards to ensure the protection of personal information, i.e., regulate the collection, use, and disclosure of personal information. Amgen is

committed to the lawful stewardship of personal information that is collected, stored and used by Amgen.[1]

5. Despite this promise and its legal obligations to safeguard the Sensitive Private Information entrusted to it, Defendant implemented inadequate data security measures and allowed the information of thousands of patients and customers to be stolen by cybercriminals.

6. On or around July 2026, a group of cybercriminals infiltrated Defendant's computer systems, accessed and exfiltrated file repositories that contained Plaintiff's and Class Members' Sensitive Private Information (the "Data Breach").

7. The Data Breach was a direct, foreseeable, and even likely result of Defendant's deficient cybersecurity practices. The wealth of publicly available information and industry warnings regarding cyberattacks attacks makes Defendant's failures all the more egregious. Defendant disregarded the rights of Plaintiff and Class Members by failing to implement proper and reasonable measures to safeguard the Sensitive Private Information in its custody, and by failing to take the available and necessary steps to prevent the unauthorized disclosure of that information.

8. While Defendant's breach of its duties led to the Data Breach, it is Plaintiff and other victims of the Data Breach that will bear the burden for years to come. The exponential cost to Plaintiff and the Class Members resulting from the Data Breach cannot be overstated. Criminals can use victims' names, birth dates, social security numbers, and addresses to open new financial accounts, rack up fraudulent charges, obtain government benefits and IDs, fabricate identities, file fraudulent tax returns, and commit medical insurance fraud well before the person whose Sensitive Private Information was stolen becomes aware of it. Any one of these instances of identity theft can have devastating consequences for the victim—causing years of damage to their credit scores, financial stability, and personal security.

[1] https://www.amgen.com/about/how-we-operate/policies-practices-and-disclosures/business-conduct/protection-of-personal-information

9. Through this lawsuit, Plaintiff seeks to hold Defendant responsible for the injuries it inflicted on Plaintiff and thousands of similarly situated individuals due to its impermissibly inadequate data security measures, and to obtain injunctive relief requiring, among other things, the implementation of security measures sufficient to protect the Sensitive Private Information that remains in Defendant's custody and control. Such injuries include: (i) lost value of Sensitive Private Information, a form of property that Defendant obtained from Plaintiff and Class members; (ii) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Sensitive Private Information; (iii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued, long term, and certain risk that unauthorized persons will access and abuse Plaintiff and Class Members' Sensitive Private Information; (v) the continued and certain increased risk that the Sensitive Private Information that remains in Defendant's possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake proper measures to protect it; (vi) theft of their Sensitive Private Information and the resulting loss of privacy rights in that information; (vii) credit freezes and unfreezes; (viii) decreased credit scores; (ix) lost work time; and (x) anxiety, annoyance, and nuisance.

10. Accordingly, Plaintiff brings this action on behalf of herself and the proposed Class for, among other things, negligence and negligence per se.

II. PARTIES

11. Plaintiff Heidi Humphreys is an adult natural person and a patient and customer of Amgen, whose Sensitive Private Information was collected, stored, and maintained by Defendant. Plaintiff Humphreys resides in Pennsylvania.

12. Defendant Amgen Inc. is a Delaware corporation with its principal executive office located at 1 Amgen Center Dr., Thousand Oaks, CA 91320.

III. JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d), because Plaintiff Humphreys and at least one member of the Class, as defined below, are citizens of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

14. Defendant is subject to personal jurisdiction in California because it maintains its principal place of business here, conducts substantial business here, and the acts and omissions giving rise to Plaintiff's claims occurred, in substantial part, in this District.

15. Venue is proper in this Court under 28 U.S.C. § 1391 because Defendant resides in this District, maintains its principal place of business in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District, including Defendant's collection, storage, and maintenance of Sensitive Private Information; the failure to implement reasonable data security measures; the operation and oversight of the systems compromised in the Data Breach; and Defendant's decisions regarding breach detection, investigation, and notification.

IV. FACTUAL BACKGROUND

A. Defendant Affirmatively Collected, Stored, and Retained Plaintiff's and Class Members' Sensitive Private Information.

16. Defendant is a multinational biotechnology company that develops, manufactures, and commercializes prescription medicines for the treatment of cancer, cardiovascular disease, inflammation, rare diseases, and other serious medical conditions.

17. In the course of providing its services, Amgen collected substantial information regarding its patients and customers, including Personally Identifiable Information like names, addresses, contact information, financial and billing information, and employment information, and Protected Health Information, including health

insurance information, health conditions, diagnoses, medical appointment and test information, prescription information, and payment and billing information.

18. Plaintiff and Class Members are individuals who entrusted, and in fact, were required to provide their Sensitive Private Information to Defendant. Plaintiff and the Class reasonably expected that Defendant would secure their Sensitive Private Information. They had good reason for their expectation— Amgen promised to do so.

19. By collecting and storing Plaintiff's and Class Members' Sensitive Private Information, Defendant assumed equitable and legal duties to implement adequate data security measures to protect and safeguard Plaintiff's and Class Members' information from unauthorized access and disclosure. Defendant was the only entity capable of securing the data in its possession against a foreseeable data breach, and Plaintiff and the Class were entirely reliant on Defendant to protect their Sensitive Private Information.

20. Defendant, however, breached these duties by implementing inadequate data security measures, creating a foreseeable risk of harm to Plaintiff and Class Members that materialized during the Data Breach, and further resulting in the access and exfiltration of Plaintiff's and Class Members' Sensitive Private Information by cybercriminals.

B. Defendant Knew the Risks of Collecting and Storing Sensitive Private Information.

21. At all relevant times, Defendant knew it was collecting and storing customer and patient Sensitive Private Information, and that as a result, its systems would be attractive targets for cybercriminals.

22. Sensitive Private Information—particularly the wide array of health-related information that Defendant collected, stored, and retained—has significant value on the criminal black market, including on the dark web, particularly in data sets containing all of the necessary building blocks to commit a variety of fraudulent schemes and identity theft. And once exposed, this information cannot be made private again.

23. Numerous sources cite dark web pricing for stolen identity credentials. For example, a single victim's personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[2] Unfortunately, law enforcement has difficulty policing dark web activity due to encryption that permits sellers and purchasers to conceal their identity.

24. While the disclosure of compilations of Sensitive Personal Information is undoubtedly harmful, even the disclosure and misuse of discrete pieces of information—especially unique government identification numbers like Social Security, passport and driver's license numbers that cannot be easily replaced—can cause significant harm. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the impacted victim, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

25. For example, the Social Security Administration warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for an identity theft victim:

> Keep in mind that a new number probably will not 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) likely 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 will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.

[2] 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; *see also*, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Mar. 31, 2024).

> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[3]

26. Because government identification numbers like Social Security numbers cannot be easily or quickly changed, victims of identity theft from data breaches often face multiple incidents of fraud over their lifetime due to the reuses of stolen data, and "may not find out that someone is using [their] [Social Security number] until [they]'re turned down for credit, or [they] begin to get calls from unknown creditors demanding payment for items [they] never bought,"[4] which highlights the long-term harms caused by the breach of such sensitive data.

27. Government agencies thus consider Social Security Numbers to be so sensitive as to warrant special considerations to ensure their security, regardless of whether they are maintained as "stand-alone [data] [or] when associated with any other identifiable information[.]"[5] The Government likewise recognizes that even partial Social Security numbers must be protected, because loss of "[t]he full or partial SSN can increase the risk of identity theft or fraud (i.e., access to bank accounts, driving records, tax and employment histories, and other private information[.]" To minimize the increase in risk of identity theft or fraud, the National Institutes of Health recommends the following measures:

a. Collect SSN as a primary identifier only if permitted by law;

b. Reduce and/or eliminate the use of SSNs not required for a business purpose;

c. Use an alternate identifier (unique, randomly generated number not derived from Sensitive Private Information);

---

[3] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[4] *Identity Theft and Your Social Security Number*, Social Security Administration (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[5] *See, e.g.*, *Frequently Asked Questions (FAQ)*, U.S. Dep't of Commerce, Office of Privacy and Open Government, https://www.commerce.gov/opog/frequently-asked-questions-faq (last visited Jan. 24, 2025).

d. Transmit SSN electronically only through an encrypted means.[6]

28. Even if cybercriminals do not gain access to a complete set of an individual's PII during a data breach, cybercriminals can cross-reference two or more sources of stolen information to marry data available elsewhere with criminally stolen data, resulting in complete and accurate dossiers on individuals. These dossiers are known as "Fullz" packages.

29. The development of "Fullz" packages means stolen information from a data breach can easily be linked to victims' 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 is not included in the Sensitive Private Information stolen in a specific incident, criminals can easily create a "Fullz" package that links that information together and sell the package at a higher price.

30. Importantly, once a cybercriminal has a "Fullz" package, cybercriminals can use it to commit a host of criminal acts including: credit card fraud, loan fraud, identity fraud, account take overs, medical identity fraud, tax refund fraud, and buy now pay later frauds.[7] Most problematic, however, is that cybercriminals in possession of a "Fullz" package "are difficult to stop with ordinary online security and ID verification measures because they possess all the information needed to get past typical authentication measures."[8]

[6] *The Privacy Pulse*, U.S. Nat'l Inst. Health (June 21, 2013), https://oma.od.nih.gov/forms/Privacy%20Documents/Privacy%20Newsletters/2013/Privacy%20Pulse%20-%20June%202013%20SSN.pdf; *see also*, https://www.dhs.gov/sites/default/files/publications/dhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf.

[7] Paige Tester, *What Are Fullz? How Hackers and Fraudsters Obtain and Use Fullz*, DataDome (Mar. 3, 2023), https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work.

[8] *Protection Against Fullz and Fraud, Integrity*, Aristotle (Apr. 18, 2022), https://integrity.aristotle.com/2022/04/protection-against-fullz-and-fraud/.

31. PHI is also highly valuable and has been referred to as a "treasure trove for criminals."[9] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[10]

32. Cyber criminals seek out PHI at greater rates than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[11] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[12]

33. According to a report released by the Federal Bureau of Investigation's (FBI) Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[13]

34. In addition, criminals can use stolen PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[14] Further, "[t]raditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[15]

---

[9] See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019),https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("What Happens to Stolen Healthcare Data") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[10] *Id.*

[11] *See* PROTENUS, 2023 Breach Barometer, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last visited Oct. 14, 2023).

[12] *Id.*

[13] *See* Andrew Steager, What Happens to Stolen Healthcare Data, HEALTHTECH MAGAZINE (Oct. 20, 2019),https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("What Happens to Stolen Healthcare Data") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[14] *Id.*

[15] Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable /23015560?seq=1.

35. Just like "Fullz" dossiers of PII are desirable to cybercriminals, stolen PII and PHI also are highly valuable because they enable cybercriminals to conduct targeted "phishing" or "spearphishing" attacks.

36. Phishing attacks are fraudulent communications—typically emails, text messages, or phone calls—designed to deceive recipients into revealing Sensitive Private Information such as login information, financial account numbers, or other highly Sensitive Private Information. These attacks often impersonate trusted institutions, including banks, government agencies, and current and former employers, and have become increasingly sophisticated in their ability to appear legitimate.[16]

37. Spearphishing is a targeted and particularly dangerous variant of phishing in which attackers use personal information about a victim—such as their name, address, employment information, Social Security number, government identification numbers, or other details—to craft highly personalized and convincing fraudulent messages. Unlike generic phishing attacks sent to mass audiences, spearphishing messages are tailored to the specific individual, dramatically increasing the likelihood that the recipient will be deceived. Information held by an employer is particularly valuable for malicious actors to use to construct such targeted attacks.[17]

38. Cybersecurity researchers and law enforcement agencies, including the FBI and the Cybersecurity and Infrastructure Security Agency (CISA), have repeatedly documented the connection between data breaches and subsequent phishing campaigns targeting affected individuals. For example, in the aftermath of the National Public Data breach in 2024, Microsoft warned consumers that the data breach created a "high likelihood" of phishing attacks using the information stolen in that breach.[18]

[16] *Spoofing and Phishing*, FBI, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing (last visited Feb. 17, 2026).
[17] *Spear Phishing vs. Phishing: What's the Difference?*, Analyst1 (Oct. 12, 2023), https://analyst1.com/spear-phishing-vs-phishing/
[18] *National Public Data breach: What you need to know*, Microsoft, https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535 (last visited Feb. 16, 2026).

39. Aside from these risks of identity theft, fraud, and phishing or spearphishing attacks, PII is also property that has monetary value to data breach victims.

40. While the economic value of individual data was leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use, market exchanges have sprung up where individual users like Plaintiff can sell or monetize her own data. For example, Nielsen Data and Mobile Computer will pay users for their data.[19] Likewise, apps such as Zynn, a TikTok competitor, pay users to sign up and interact with the app.[20]

41. There are numerous examples of this kind of market, which is growing more robust as information asymmetries are diminished when users discover how their data is being covertly intercepted, collected, used, and disclosed.

42. According to an essay published by the Centre for International Governance Innovation:

> The social and economic importance of personal data is well understood. Personal data — typically defined as "information about an identifiable individual" — is central to a person's identity and can reveal intimate details about them. For businesses and governments that collect personal data, this information is often necessary to provide goods or services to specific individuals. However, personal data can also be used in the design and creation of goods or services. For example, such data can be used to create profiles or to drive targeted advertisements. Personal data is used in massive quantities to train artificial intelligence (AI) systems; it is also important to a variety of research activities.[21]

43. In other words, a successful cyberattack leaves criminals with a lucrative and readily monetized supply of Sensitive Private Information—and deprives its victims of the exclusive use of their own information.

---

[19] Kevin Mercandante, *Ten Apps for Selling Your Data for Cash, Best Wallet Hacks* (June 10, 2020), https://wallethacks.com/apps-for-selling-your-data/.
[20] Jacob Kastrenakes, *A new TikTok Clone hit the top of the App Store by paying users to watch videos*, The Verge (May 29, 2020), https://www.theverge.com/2020/5/29/21274994/zynn-tiktokclone-pay-watch-videos-kuaishou-bytedance-rival.
[21] Teresa Scassa, *Different Perspectives on Notions of Value The shifting Value of Personal Data* (Nov. 12, 2024), https://www.cigionline.org/articles/the-shifting-value-of-personal-data/ (last visited Mar. 2, 2026).

44. The value of this information has led to a marked increase in the number of data breaches in the United States, in particular in the healthcare sector.

45. In 2024, at least 725–742 large healthcare breaches (affecting 500+ individuals) were reported to the U.S. Department of Health and Human Services' Office for Civil Rights.[22] And in 2025, roughly 600–640 large breaches reported by year's end, averaging about 57–63 breaches per month.[23]

46. Because of the enormous number of healthcare data breaches and their publicity, Defendant knew or should have known that the Sensitive Private Information it collected and retained—including PII and PHI—was highly sensitive and of significant value to cybercriminals, as this information is routinely bought, sold, and exploited on criminal marketplaces, including on the dark web, where it can be used to commit identity theft, financial fraud, medical identity theft, tax fraud, and other crimes.

47. Likewise, the documented increase in cyberattacks, combined with increasing monetary incentives that heighten the risk of future attacks, was widely known to the public and to anyone in Defendant' industry, including Defendant, at the time of the Data Breach.

48. Defendant was therefore on notice of the risk of cyberattack and misuse of data in its custody well before the Data Breach. Highly publicized data breaches involving similarly situated entities had already demonstrated that centralized repositories of health-related data are prime targets for cybercriminals seeking to exfiltrate and monetize Sensitive Private Information.

49. Plaintiff and Class Members relied on Defendant to keep their Sensitive Private Information confidential and secure, to use their information for business purposes only, to delete their information when it was no longer reasonably necessary to retain, and to make only authorized disclosures of their information.

---

[22] https://www.hipaajournal.com/2025-healthcare-data-breach-report/?utm_source=chatgpt.com

[23] *Id.*

50. By obtaining, collecting, and storing Plaintiff's and Class Members' Sensitive Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' Sensitive Private Information from foreseeable risks of disclosure to unauthorized parties. Defendant agreed to and undertook legal duties to securely store and maintain the Sensitive Private Information of Plaintiff and Class Members.

51. Indeed, as demonstrated by the foregoing, Defendant's collection, storage, and retention of Sensitive Private Information created a foreseeable and substantial risk of precisely the type of harm suffered by Plaintiff and Class Members, including loss of control over their personal information, increased risk of identity theft and fraud, actual misuse of their PII and PHI, and the need for ongoing mitigation measures.

C. Defendant Failed to Protect that Sensitive Private Information, resulting in the Data Breach.

52. On or around July 2026 unauthorized actors gained access to Defendant's computer systems and acquired files containing Sensitive Private Information. The incident resulted from Defendant's failure to adequately secure its networks, systems, and data against foreseeable cyber threats. As a result of the intrusion, cybercriminals were able to access and potentially exfiltrate Sensitive Private Information belonging to affected individuals.

53. The information compromised in the breach included, among other things, patient protected health information and the individually identifying information of patients and customers. Such information is highly valuable to identity thieves and can be used to commit fraud, identity theft, medical identity theft, and other forms of misuse. Individuals whose information was exposed therefore face an ongoing and heightened risk of identity theft, financial fraud, and other harms resulting from the breach.

54. On July 31, 2026, Amgen notified the Securities and Exchange Commission of the data breach through an 8-K filing.

D. The Data Breach and the resulting harm was entirely foreseeable and Defendant failed to protect against it or to minimize its impact.

55. The risk of a data breach was well known and foreseeable to Defendant. As set forth *supra*, Sensitive Private Information of the type Defendant maintained is a prime target for cybercriminals, and ransomware attacks against large companies and centralized data storage systems were widespread and escalating well before the intrusion.

56. Despite this known risk, Defendant failed to implement reasonable cybersecurity safeguards appropriate to the nature and scope of the data it collected and retained.

57. Cybersecurity firms and federal agencies have promulgated a series of best practices that should be implemented by companies that handle or facilitate the handling of personal information like that Defendant collected and kept, including, at minimum: establishing secure password and authentication procedures for employees; building secure networks by setting up network protection tools like firewalls and constantly monitoring for and patching vulnerabilities; monitoring active and inactive IP addresses, whitelisting software, and monitoring suspicious traffic on their networks; encrypting sensitive data using robust encryption algorithms; limiting access to data to only relevant staff; and properly training staff regarding password hygiene, phishing attacks, and social engineering attacks.[24]

58. The FTC has issued numerous guides for business outlining reasonable data and cyber security practices to diminish data breaches and the resulting harm to

[24] *Customer Data Security: Best Practices for Data Privacy*, CDP, https://cdp.com/articles/customer-data-security-best-practices/; NIST, *Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information*, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf

consumers and financial institutions, which it believes should be factored into all business decision-making.[25]

59. The FTC's 2016 publication Protecting Personal Information: A Guide for Business—which the agency re-endorsed in October 2023—established guidelines for fundamental data and cyber security principles and practices for business.[26] The guidelines note businesses should, among other best practices:

a. Protect the personal customer and consumer information that they keep;

b. Properly dispose of personal information that is no longer needed;

c. Encrypt information stored on computer networks;

d. Understand their network's vulnerabilities; and

e. Implement policies to correct security problems[27]

60. The guidelines further recommend that businesses implement an array of specific methods to protect their systems, such as:

a. Using an intrusion detection system to expose a breach as soon as it occurs;

b. Monitoring all incoming traffic for activity indicating someone is attempting to hack the system;

c. Watching for large amounts of data being transmitted from the system; and

d. Having a response plan ready in the event of a breach.[28]

---

[25] *Start with Security: A Guide for Business* at 2, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[26] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business. *See also Start with Security: A Guide for Business*, FTC (October 2023) (reiterating the principles underlying *Protecting Personal Information: A Guide for Business* and acknowledging "[t]hreats to data may transform over time, but the fundamentals of sound security remain constant.)

[27] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[28] *Id*.

61. For example, Defendant is prohibited by the FTC Act from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' Sensitive Private Information is an "unfair practice" in violation of the FTC Act.

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer data, including employee and human resources data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. While Defendant is prohibited by the FTC Act from engaging in "unfair or deceptive acts or practices in or affecting commerce," Defendant nonetheless failed to implement reasonable and appropriate security measures to protect against unauthorized access to its employees confidential Sensitive Private Information.

63. Further, the National Institute of Standards in Technology ("NIST") publishes specific recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[29] Defendant failed to adhere to NIST guidance.

64. For example, NIST recommends that, to prevent security breaches through phishing attacks, companies should: require employees to practice regular exercises in no-notice social engineering attempts to collect information and gain unauthorized access to company systems; educate employees on the adverse impact of opening malicious email attachments; provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining; and monitor emerging

[29] *Security and Privacy Controls for Information Systems and Organizations*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last visited Feb. 13, 2026).

vulnerabilities (like new social engineering techniques) and implement procedures to mitigate the risks of those vulnerabilities.[30]

65. NIST further recommends that, to limit the impact of a data breach, organizations must dispose of information in its custody or control once it is no longer needed.[31]

66. Defendant is covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (see 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

67. These rules establish national standards for the protection of patient information, including personal health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

68. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[32]

69. HIPAA requires that businesses implement appropriate safeguards for this information.[33] Specifically, HIPAA security standards require organizations to "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information."[34]

70. Defendant implemented inadequate security measures and failed to comply with industry standards to prevent social engineering and ransomware attacks, specifically by:

---

[30] *Id.* at 60-61.
[31] *Id.* at 352.
[32] 45 C.F.R. § 164.502.
[33] 45 C.F.R. § 164.540(c)(1).
[34] 45 C.F.R. § 164.306.

a. failing to adequately train employees on phishing attacks, social engineering attacks, and ransomware attacks;

b. failing to conduct simulated phishing campaigns to test readiness;

c. failing to implement procedures to mitigate the risk of social engineering and ransomware attacks;

d. failing to implement advanced email security platforms with phishing detection;

e. failing to conduct real-time URL and attachment scanning;

f. failing to implement Zero Trust network architecture;

g. failing to implement endpoint detection and response (EDR) systems;

h. failing to adequately monitor its systems for suspicious activity;

i. failing to adequately encrypt or otherwise secure Sensitive Personal Information in its custody;

j. failing to detect unauthorized access in a timely manner; and

k. failing to promptly contain the intrusion once it occurred.

71. Defendant also failed to implement reasonable and appropriate data minimization and retention practices, particularly for the type of data it chose to collect and keep. Defendant retained vast quantities of Sensitive Private Information—long after such information was reasonably necessary for legitimate business purposes, thereby increasing the scope and severity of the Data Breach.

72. Reasonable data security measures—such as network segmentation, access controls, employee training, encryption of sensitive data, intrusion-detection systems, advanced email security platforms with phishing detection, and regular vulnerability testing—were available, widely adopted in Defendant's industry, and necessary to protect the Sensitive Private Information entrusted to Defendant.

73. Defendant failed to implement or properly maintain these reasonable measures, despite representing that it would safeguard Sensitive Private Information and despite its obligations under applicable laws, regulations, and industry standards.

74. As a direct and proximate result of Defendant's data security failures, unauthorized actors were able to access Defendant's systems, exfiltrate Sensitive Private Information, and publish that information on the dark web, causing the injuries alleged herein.

E. The Data Breach Put Plaintiff and Class Members at Imminent Risk of Fraud, Identity Theft, and other Cybercrimes.

75. Defendant's failure to keep Plaintiff's and Class Members' Sensitive Private Information secure has severe ramifications.

76. Given the nature of the Sensitive Private Information stolen in the Data Breach, hackers can commit identity theft, financial fraud, healthcare fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future.

77. Plaintiff has already suffered injury, including misuse of the information stolen in the Data Breach, and she faces an imminent and substantial risk of further injury including identity theft and fraud and related cybercrimes due to the Data Breach.

78. Criminal law also recognizes the value of Sensitive Private Information by imposing harsh prison sentences for those who steal this data. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of Sensitive Private Information by: (1) demanding a ransom or blackmail payment for its destruction, (2) using Sensitive Private Information to commit fraud or identity theft, or (3) selling Sensitive Private Information to other cybercriminals on the black market and on the dark web.

79. Once cybercriminals start committing fraud and other identity theft-related crimes using a victim's Sensitive Private Information, the disruption to the victim's life can be catastrophic. A study by the Identity Theft Resource Center ("ITRC") found that, among individuals who experienced fraudulent use of their Sensitive Private Information, nearly all of them had experienced some form of costs or other harm in their lives,

including having to borrow money, being forced out of their home or residence, and being unable to care for their family.[35]

80. Further, although the theft of Sensitive Private Information creates an imminent risk of becoming a victim of identity theft and fraud, malicious actors often wait months or years to use the PII obtained in data breaches. GAO determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[36] During this delay, victims often become complacent and less diligent in monitoring their accounts after a significant period has passed.

81. Cybercriminals will also re-use stolen Sensitive Private Information, meaning individuals can be the victim of several cybercrimes stemming from a single data breach.

82. Beyond all of the injuries described, events like the Data Breach also have a deep psychological impact on their victims:

> In some ways, a cyber attack can feel like the digital equivalent of getting robbed, with a corresponding wave of anxiety and dread. Anxiety, panic, fear, and frustration—even intense anger—are common emotional responses when experiencing a cyber attack. While expected, these emotions can paralyze you […].[37]

V. PLAINTIFFS' EXPERIENCES

83. Plaintiff Huphreys is a current or former patient and customer of Defendant.

84. Plaintiff Huphreys's Sensitive Private Information was accessed and exfiltrated in the Data Breach.

---

[35] Identity Theft Resource Center, *Identity Theft Resource Center 2025 Consumer Impact* Report (October 2025), https://www.idtheftcenter.org/wp-content/uploads/2025/10/The-2025-ITRC-Consumer-Impact-Report.pdf at 16.

[36] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm.

[37] Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass (Aug. 17, 2022), https://blog.lastpass.com/posts/the-psychological-impact-of-cyber-attacks.

85. Plaintiff Huphreys would not have entrusted her information with Defendant if she knew of Defendant's deficient data security practices. Plaintiff Huphreys only allowed Defendant to maintain, store, and use her Sensitive Private Information because she reasonably expected that Defendant would use basic security measures to protect the information entrusted to it and prevent its access by unauthorized third parties.

86. As a result of the Data Breach, Plaintiff Huphreys has experienced attempts at fraudulent accounts being opened in her name.

87. As a result of the Data Breach, Plaintiff Huphreys has received notice that her information is on the dark web.

88. As a result of the Data Breach, Plaintiff Huphreys has experienced an increase in spam calls and text messages.

89. As a result of the Data Breach, Plaintiff Huphreys has experienced an immediate loss of privacy the moment her Sensitive Private Information was accessed and exfiltrated without her authorization.

90. As a result of the Data Breach, Plaintiff Huphreys has experienced loss of time spent responding to the Data Breach.

91. Plaintiff Huphreys has had to spend time and effort mitigating the risk of harm caused by the Data Breach, including the following: gathering information about the data breach, monitoring her accounts, and responding to attempts to open fraudulent accounts in her name.

92. As a result of the disclosure of Sensitive Private Information to unauthorized individuals due to the Data Breach, Plaintiff Huphreys has suffered an invasion of privacy.

93. As a result of the Data Breach, Plaintiff Huphreys has suffered anxiety, stress, and emotional distress arising from the loss of control over her Sensitive Private Information and the ongoing risk of misuse.

VI. CLASS ACTION ALLEGATIONS

94. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure.

A. Class Definitions

95. Plaintiff seeks to represent the following Class (collectively, the "Classes"):

> **Nationwide Class**
> All persons residing in the United States whose Sensitive Private Information was accessed, exfiltrated, or otherwise compromised in the Amgen data breach that occurred in or around July 2026 (the "Nationwide Class").

96. Excluded from the Class is Defendant; any entity in which Defendant has a controlling interest; Defendant's officers, directors, employees, legal representatives, successors, and assigns; and the judicial officer assigned to this case and members of the judicial officer's immediate family.

97. Plaintiff reserves the right to amend or modify the Class Definition as discovery and further investigation reveal additional facts.

B. Numerosity

98. The Class is so numerous that joinder of all members is impracticable. Upon information and belief, the Data Breach compromised the Sensitive Private Information of tens of thousands of individuals.

C. Commonality

99. Questions of law and fact are common to the Class and predominate over questions affecting only individual members. Common questions include, but are not limited to:

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

b. Whether Defendant were negligent in collecting and storing Plaintiff's and Class Members' Sensitive Private Information;

c. Whether Defendant had duties not to disclose the Sensitive Private Information of Plaintiff and Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' Sensitive Private Information;

e. Whether Defendant failed to adequately safeguard the Sensitive Private Information of Plaintiff and Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' Sensitive Private Information;

g. 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;

h. Whether Defendant failed to timely detect, contain, and investigate the Data Breach;

i. Whether Defendant failed to timely and adequately notify Plaintiff and Class Members of the Data Breach;

j. Whether Defendant's acts and omissions caused Plaintiff's and Class Members' injuries;

k. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of the Data Breach and Defendant's wrongful conduct; and

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

D. Typicality

100. Plaintiff's claims are typical of the claims of the Class because Plaintiff and all Class Members were subjected to the same Data Breach, had their Sensitive

Private Information compromised as a result of Defendant's uniform conduct, suffered similar injuries arising from Defendant's failures, and Plaintiff's and Class Members' claims are premised on the same legal theories.

E. Adequacy

101. Plaintiff will fairly and adequately protect the interests of the Classes, because Plaintiff's interests are not antagonistic to those of the Class that Plaintiff seeks to represent, and Plaintiff is committed to vigorously prosecuting this action.

102. Plaintiff has retained counsel that are competent and experienced in complex class action litigation, data breach cases, and consumer and privacy protection matters, have adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed, and are committed to adequately representing the interests of the Classes.

F. Predominance and Superiority—Rule 23(b)(3)

103. Common questions of law and fact predominate over any questions affecting only individual members of the Class. Defendant engaged in a common course of conduct that gives rise to Plaintiff's and Class Members' claims, and this litigation will turn on similar or identical violations, business practices, and injuries. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages are common to Plaintiff and each member of the Classes. If Defendant breached its duties and failed to protect Plaintiff's and Class Members' PII from theft and misuse, then Plaintiff and each Class Member suffered damages by that conduct.

104. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation or joinder of all Class Members would be impracticable and inefficient given the number of affected individuals and the common factual and legal issues presented. The proposed class action presents fewer management difficulties than individual litigation, and provides

the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

G. Injunctive and Declaratory Relief – Rule 23(b)(2)

105. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief and corresponding declaratory relief with respect to the Class as a whole.

106. As demonstrated by the Data Breach, Defendant has failed to implement and maintain reasonable administrative, technical, and physical safeguards to protect Plaintiff's and Class Members' Sensitive Private Information, and has demonstrated an inability or unwillingness to do so absent judicial intervention.

107. Plaintiff and Class Members therefore remain at a continuing and imminent risk of harm because their Sensitive Private Information remains in Defendant's possession, custody, or control, and Defendant's systems have already been shown to be vulnerable to compromise.

108. Plaintiff therefore seeks injunctive relief requiring Defendant to implement reasonable and appropriate data security measures, improve breach detection and response protocols, limit the collection and retention of Sensitive Private Information to that which is reasonably necessary for legitimate business purposes and delete all data that is no longer reasonably necessary for Defendant to have in its possession, custody and control, provide appropriate data security training for employees, undergo periodic third-party security assessments, and comply with applicable data protection and notification obligations to prevent Plaintiff's significant, imminent, and ongoing risk of future harm.

VII. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

109. Plaintiff restates and realleges the allegations contained in paragraphs 1-108 as if fully set forth herein.

110. Defendant owed Plaintiff and Class Members a duty to exercise reasonable care in collecting, storing, maintaining, and safeguarding their Sensitive Private Information to prevent that information from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

111. Defendant's duty arose from Defendant's affirmative collection of Plaintiff's and Class Members' Sensitive Private Information, exclusive possession and control of that information, the foreseeability of harm from unauthorized access, Defendant's representations and practices regarding data security, and Defendant's obligations under applicable laws, regulations, and industry standards.

112. Defendant has full knowledge of the sensitivity and value of the Sensitive Private Information that it collected from Plaintiff and Class Members, and the type of harm that Plaintiff and Class Members would suffer if their Sensitive Private Information was stolen and/or wrongfully disclosed.

113. Defendant's duty to use reasonable care arose from several other sources, including but not limited to those alleged herein.

114. Defendant further had common law duties to prevent foreseeable harm to Plaintiff and Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Defendant knew that it was collecting and maintaining highly Sensitive Private Information, that its computing systems and data storage architecture were vulnerable to unauthorized access, and that Defendant's systems would be targeted hackers for the purpose of stealing and misusing the troves of highly valuable Sensitive Private Information that it collected, stored, and retained.

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

116. Additionally, Defendant assumed a duty to Plaintiff and the Class to protect their sensitive Personal Information. Defendant represented to providers and others that it would comply with HIPAA to implement measures to reasonably safeguard the patient information within their possession. As such, when individuals and entities provided Defendant with Plaintiff's and the Class's Sensitive Personal Information and Defendant accepted and stored that data (for its own purposes and to its own financial benefit), Defendant assumed a duty to protect that Personal Information.

117. Defendant also had a duty to safeguard the Sensitive Private Information of Plaintiff and Class Members and to promptly notify them of a breach under various state laws and statutes that require Defendant to reasonably safeguard sensitive Private Information, as detailed herein.

118. Defendant's duty to exercise reasonable care regarding Plaintiff's and Class Member's Sensitive Private Information included, among other things: (a) designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class Members' personal information in Defendant's possession was adequately protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) properly training employees to prevent breaches of its systems; and (d) maintaining security measures consistent with industry standards, including regularly updating, patching, and evaluating security measures.

119. Defendant's duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a

special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

120. Defendant also had a duty to provide timely, adequate notification of a data breach so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles; avoid unauthorized charges on their credit or debit card accounts; monitor their account information and credit reports for fraudulent activity; contact their banks or other financial institutions that issue their credit or debit cards; obtain credit monitoring services; contact their health insurers or governmental health insurance providers; and take other steps to mitigate or ameliorate the damages caused by Defendant's misconduct. Defendant was the only entity that had sufficient knowledge to properly provide this notice.

121. Defendant breached the duties it owed to Plaintiff and Class Members alleged above and, thus, was negligent in failing to do so. Defendant breached these duties by, among other things: (a) implementing inadequate security systems, protocols and practices that were insufficient to protect the Sensitive Private Information of Plaintiff and Class Members; (b) failing to adequately monitor its systems for suspicious activity; (c) failing to timely detect, investigate, and contain the Data Breach and other unauthorized activity on its system while it was ongoing; (d) implementing inadequate and unreasonable access controls, intrusion-detection, and data-protection measures; (e) implementing security systems that did not comply with industry standards; (f) failing to comply with regulations protecting the Sensitive Private Information at issue during the period of the Data Breach; (f) over-retaining Sensitive Private Information for longer than reasonably necessary; and (g) inadequately disclosing the Data Breach to Plaintiff and Class Members in an unreasonably delayed manner.

122. Defendant's acts and omissions fell below the standard of care that an entity entrusted with Sensitive Private Information would reasonably exercise under similar circumstances.

123. As a direct and proximate result of Defendant's negligence, unauthorized actors accessed and exfiltrated Plaintiff's and Class Members' Sensitive Private Information, causing the injuries and damages alleged herein.

124. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Sensitive Private Information would not have been compromised.

125. Defendant's failure to take proper security measures to protect the Sensitive Private Information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' Sensitive Private Information. As the entity collecting and storing Plaintiff's and Class Members' Sensitive Private Information, Defendant was in the best position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

126. Plaintiff and Class Members were foreseeable victims of Defendant's inadequate data security practices, and it was also foreseeable that Defendant's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as alleged in this Complaint.

127. Defendant's negligence was therefore a substantial factor in causing Plaintiff's and Class Members' injuries, and Plaintiff and Class Members' injuries are the direct and proximate result of Defendant's wrongful and negligent conduct.

128. Plaintiff's and Class Members' injuries include: (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the their privacy and the confidentiality of the stolen Sensitive Private Information and loss of control over their Sensitive Private Information which occurred the moment their Sensitive Private Information was accessed, viewed and exfiltrated without authorization; (c) the illegal sale of the compromised Sensitive Private Information on the black market; (d) the present and continuing threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (e) mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes;

(f) the time spent in response to the Data Breach reviewing bank statements, credit card statements, financial account statements, credit reports, health insurance statements, and other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores and ratings; (i) emotional distress; (j) their lost work time; (k) the lost value of the Sensitive Private Information; (l) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; and (m) nominal and general damages and other economic and non-economic harm suffered.

129. Plaintiff and Class Members seek all relief available under law, including compensatory and consequential damages, restitution, injunctive relief requiring Defendant to implement reasonable data security measures and compliance programs, and such other relief as the Court deems just and proper.

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

130. Plaintiffs reallege and incorporate by reference the foregoing allegations in paragraphs 1-108 as if fully set forth herein.

131. Defendant owed a duty to Plaintiff and Class Members to keep their Sensitive Private Information secure, arising under FTC Act.

132. Specifically, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to use reasonable measures to protect Sensitive Private Information. Various FTC publications and orders further form the basis of Defendant's duty.

133. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Sensitive Private Information and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Private Information it obtained and stored and the foreseeable consequences of a data breach involving the highly Sensitive Private Information that

Defendant collected, stored, and maintained, including the damages that would result to Plaintiff and Class Members.

134. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

135. Defendant is a HIPAA covered entity.

136. Plaintiff and the Class, as patients, are within the class of people HIPAA was designed to protect and HIPAA was intended to protect Plaintiff and the Class against the type of harm that occurred, namely, unauthorized access to Plaintiff's and the Class's medical information.

137. Defendant's implementation of inadequate data security failed to comply with HIPAA.

138. Defendant's violations of Section 5 of the FTC Act as well as HIPAA constitutes negligence *per se*.

139. Defendant violated its duties by, among other things, inadequate security systems, protocols and practices that were insufficient to protect the Sensitive Private Information of Plaintiff and Class Members, and by failing to timely and adequately notify Plaintiff and Class Members of the Data Breach.

140. Defendant's violations constitute negligence per se because Defendant violated laws designed to protect a specific class of persons—Plaintiff and Class Members—from a particular type of harm that Defendant's conduct caused.

141. Plaintiff and Class Members suffered injuries of the type the statutes were intended to prevent, including: (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the their privacy and the confidentiality of the stolen Sensitive Private Information and loss of control over their Sensitive Private Information which occurred the moment their Sensitive Private Information was accessed, viewed and exfiltrated without authorization; (c) the illegal sale of the compromised Sensitive Private Information on the black market; (d) the present and continuing threat of identity theft crimes, fraud, and other misuse, resulting

in monetary loss and economic harm; (e) mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (f) the time spent in response to the Data Breach reviewing bank statements, credit card statements, financial account statements, credit reports, health insurance statements, and other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores and ratings; (i) emotional distress; (j) their lost work time; (k) the lost value of the Sensitive Private Information; (l) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; and (m) nominal and general damages and other economic and non-economic harm suffered.

142. Defendant's violations of these statutes were a direct and proximate cause of Plaintiff's and Class Members' injuries and damages.

143. As a result of Defendant's negligence per se, Plaintiff and Class Members are entitled to all relief available under law, including compensatory and consequential damages, statutory damages where available, injunctive relief, and such other relief as the Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class, respectfully request that the Court enter judgment in their favor and against Defendant, and grant the following relief:

A. Certify this action as a class action pursuant to Federal Rule of Civil Procedure 23, appoint Plaintiff as Class Representatives, and appoint Plaintiff's counsel as Class Counsel;

B. Declare that Defendant breached its duties to Plaintiff and Class Members, and that Defendant's acts and omissions described herein violate Plaintiff's and Class Members' legal rights;

C. Grant injunctive relief to prohibit Defendant from unlawfully retaining Plaintiff's and the Class Members' Sensitive Private Information and

continuing to engage in the unlawful acts, omissions, and practices described herein, and requiring Defendant to implement improved security procedures and measures, including, inter alia:

1. Requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Sensitive Private Information;
2. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
3. Requiring Defendant to adequately train employees on phishing attacks, social engineering attacks, and ransomware attacks;
4. Requiring Defendant to implement procedures to mitigate the risk of social engineering and ransomware attacks, including implementing advanced email security platforms with phishing detection, conducting real-time URL and attachment scanning, implementing Zero Trust network architecture, and implementing endpoint detection and response (EDR) systems;
5. Requiring Defendant to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
6. Requiring Defendant to implement a system to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting Sensitive Private Information;
7. Requiring Defendant to implement, maintain, regularly review and revise as necessary, a threat management program designed to

appropriately monitor information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

D. Award Plaintiff and Class Members statutory damages, statutory penalties actual damages, compensatory damages, and nominal damages, as allowable by law and in an amount to be determined;

E. Order restitution, disgorgement, and all other equitable monetary relief necessary to remedy Defendant's unjust enrichment;

F. Order Defendant to provide appropriate notice, remediation, and ongoing protective services reasonably necessary to mitigate future harm to Plaintiff and Class Members whose Sensitive Private Information was compromised;

G. Award Plaintiff and Class Members their reasonable attorneys' fees, costs, and expenses incurred in this action, as permitted by law.

H. Award pre-judgment and post-judgment interest as allowed by law;

I. Enter all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Grant such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Respectfully submitted,

Dated: August 6, 2026

/s/ Caleb Marker

Caleb Marker (SBN 269721)
ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780 Telephone
(877) 500-8781 Facsimile
caleb.marker@zimmreed.com

MaryBeth V. Gibson (*pro hac vice* forthcoming)
Gibson Consumer Law Group, LLC
4279 Roswell Road
Suite 208-108

Atlanta, GA 30342
Telephone: (678) 642-2503
marybeth@gibsonconsumerlawgroup.com

Attorneys for Plaintiff and the Proposed Class