

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA**

In re Medtronic Data Sec. Incident Litig.

Case No. 26-cv-2406 (DWF/DLM)

**PLAINTIFFS' CONSOLIDATED
CLASS ACTION COMPLAINT**

This Document Relates to All Actions

Plaintiffs Chris Rath, Tiffani Corvia, Robin Jennings, Richard Loughry, Adam McLain, Nancy Buckner, Lisa Riley, Jeffrey Kennedy, Vivian Lindley, Anthony Spano, David Holmes, and Linda Egbert (“Plaintiffs”), individually and on behalf of all others similarly situated, and on behalf of the general public, bring this Consolidated Class Action Complaint, against Defendant Medtronic, Inc. (“Defendant”) based on personal knowledge and the investigation of counsel, and allege as follows:

I. INTRODUCTION

1. With this action, Plaintiffs seek to hold Defendant responsible for the harms it caused Plaintiffs and similarly situated persons in the preventable data breach of Defendant’s inadequately protected computer network (the “Data Breach”).

2. Defendant is a global leader in healthcare technology, operating in over 150 countries with more than 95,000 employees.¹ Founded in 1949, the company focuses on engineering medical devices that treat over 70 health conditions, ranging from cardiac, neurovascular, and surgical robotics to insulin pumps.²

3. On April 17, 2026, the notorious ransomware gang “ShinyHunters” listed

¹ *Key Facts*, MEDTRONIC, <https://www.medtronic.com/bd-en/our-company/key-facts.html> (last accessed July 9, 2026).

² *Id.*

Defendant on its leak website on the Dark Web, stating that they obtained more than 9 million records containing highly sensitive Personally Identifiable Information (“PII”) and Protected Health Information (“PHI”) (collectively, “Personal Information”) from Defendant’s IT network.³

4. On or around April 21, 2026, Defendant confirmed it experienced the Data Breach and indicated its investigation into the nature and scope of the Data Breach was ongoing.⁴

5. However, it was not until approximately July 1, 2026, that Defendant began formally notifying those affected by the Data Breach and providing any details about its scope (“Breach Notice”), confirming that it spanned a full week and affected the names, contact information, dates of birth, Social Security numbers, and health-related information of its current and former patients, employees, and customers.⁵ A sample of the Breach Notice is attached as Exhibit A.

6. Defendant’s Breach Notice obfuscated the nature of the Data Breach and the threat it posed by failing to inform victims of critical details, including, *inter alia*, how many people were impacted, what vulnerabilities were exploited, and why Defendant delayed three months before notifying victims that hackers had gained access to their highly sensitive Personal Information.

7. In its ordinary course of business operations, Defendant collects and stores a

³ Eduard Kovacs, *Medtronic Hack Confirmed After ShinyHunters Threatens Data Leak*, SECURITYWEEK (Apr. 28, 2026), <https://www.securityweek.com/medtronic-hack-confirmed-after-shinyhunters-threatens-data-leak/> (last accessed July 22, 2026).

⁴ Alessandro Mascellino, *Medtronic Confirms Data Breach After ShinyHunters Claims*, INFOSECURITY MAGAZINE (Apr. 28, 2026), <https://www.infosecurity-magazine.com/news/medtronic-data-breach-shinyhunters/> (last accessed July 22, 2026).

⁵ *Medtronic statement on unauthorized system access*, MEDTRONIC, <https://news.medtronic.com/Medtronic-statement-on-unauthorized-system-access> (last updated June 29, 2026); *Notice of Data Breach*, <https://oag.ca.gov/system/files/Consumer%20Letter%20-%20Exhibit%20A%20%281%29.pdf> (last accessed July 9, 2026).

substantial amount of sensitive data.

8. By taking possession and control of Plaintiffs' and Class members' Personal Information, Defendant assumed a duty to securely store and protect that Personal Information.

9. Defendant breached this duty and betrayed the trust of Plaintiffs and Class members by failing to properly safeguard and protect their Personal Information, thus enabling cybercriminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

10. Defendant's misconduct—failing to implement adequate and reasonable measures to protect Plaintiffs' and Class members' Personal Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices in place to safeguard the Personal Information, and failing to provide timely and adequate notice of the Data Breach—caused substantial harm and injuries to Plaintiffs and Class members across the United States.

11. Due to Defendant's negligence and failures, cybercriminals obtained and now possess everything they need to commit personal identity theft and wreak havoc on the financial and personal lives of thousands of individuals, for decades to come.

12. Plaintiffs bring this Consolidated Class Action lawsuit to hold Defendant responsible for its negligent failure to use statutorily required or reasonable industry cybersecurity measures to protect Class members' Personal Information.

13. As a result of the Data Breach, Plaintiffs and Class members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains, Plaintiffs and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiffs and Class members are now forced to deal with the danger of criminals possessing, using, and distributing their Personal Information.

14. Additionally, Plaintiffs and Class members have already lost time and money responding to and mitigating the impact of the Data Breach. Those efforts are continuous and ongoing.

15. Plaintiffs bring this action individually and on behalf of the Class and seek actual damages and restitution. Plaintiffs also seek declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court deems necessary and proper.

II. THE PARTIES

16. Plaintiff Rath is a natural person and citizen of Alexandria, Minnesota, where he intends to remain.

17. Plaintiff Corvia is a natural person and citizen of Fridley, Minnesota, where she intends to remain.

18. Plaintiff Jennings is a natural person and citizen of Burkeville, Virginia, where she intends to remain.

19. Plaintiff Loughry is a natural person and citizen of Potter Valley, California, where he intends to remain.

20. Plaintiff McLain is a natural person and citizen of Athens, Alabama, where he intends to remain.

21. Plaintiff Buckner is a natural person and citizen of Hawthorn, Florida, where she intends to remain.

22. Plaintiff Riley is a natural person and citizen of Clear Lake, Minnesota, where she intends to remain.

23. Plaintiff Kennedy is a natural person and citizen of Okeechobee, Florida, where he

intends to remain.

24. Plaintiff Lindley is a natural person and citizen of Houston, Texas, where she intends to remain.

25. Plaintiff Spano is a natural person and citizen of Yuma, Arizona, where he intends to remain.

26. Plaintiff Holmes is a natural person and citizen of Sheridan, Arkansas, where he intends to remain.

27. Plaintiff Egbert is a natural person and citizen of Santee, California, where she intends to remain.

28. Defendant Medtronic USA, Inc., is a wholly owned subsidiary of Medtronic, Inc. It is a Minnesota Corporation with its principal place of business in Fridley, Anoka County, Minnesota.

III. JURISDICTION AND VENUE

29. Plaintiffs incorporate by reference all allegations of the preceding and forthcoming paragraphs as though fully set forth herein.

30. The Class Action Fairness Act (CAFA) confers diversity jurisdiction to a class action where (1) the “matter in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs,” and (2) “*any* member of a class of Plaintiff is a citizen of a State different from *any* defendant.” 28 U.S.C. § 1332(d)(2) (emphasis added).

31. This Court has diversity jurisdiction over this action under CAFA, 28 U.S.C. § 1332(d), because this is a class action consisting of more than 100 class members, the amount in controversy exceeds \$5,000,000 exclusive of interest and costs, and at least one member of the Class is a citizen of a state that differs from any Defendant.

32. This Court has personal jurisdiction over Defendant because Defendant conducts

business in this District, maintains its principal place of business in this District, and has sufficient minimum contacts with the State of Minnesota.

33. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and therefore Defendant resides in this District pursuant to 28 U.S.C. § 1391(c)(2). Venue is further proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims also occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business

34. Medtronic is the world's largest medical device company by revenue. From pacemakers to surgical robots, Defendant employs more than 95,000 individuals across 150 countries. Defendant serves around 79 million patients annually and had \$33.5 billion in revenue in the 2025 fiscal year.

35. In the regular course of its business, Defendant collects and stores vast quantities of Personal Information. Upon information and belief, Plaintiffs' and Class members' Personal Information was collected, stored, and maintained by Defendant. Defendant was entrusted with, and obligated to safeguard, the Personal Information of Plaintiffs and Class members in accordance with all applicable laws.

36. Defendant's website provides: "Our customer may sometimes be a hospital, physician, or other healthcare provider; at other times, patients themselves are our customers or clinical trial participants. We obtain the patient information on which our business depends in accordance with applicable laws"⁶

⁶ *U.S. patient privacy principles*, <https://www.medtronic.com/en-us/our-company/governance/principles-ethics/us-patient-privacy-principles.html> (last accessed July 9, 2026).

37. Defendant further publicly claimed: “We maintain appropriate physical, technical and administrative security standards and procedures to safeguard our patient data and systems. Our employees are educated on the importance of our privacy and security policies and must comply with them. Employees are permitted to access and use only the patient information they need to perform their job duties.”⁷

38. By obtaining, collecting, using, and deriving a benefit from Plaintiffs’ and Class members’ Personal Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting that Personal Information from disclosure.

39. Plaintiffs and Class members reasonably relied on Defendant’s representations regarding privacy and data security—including its public statements concerning the safeguarding of patient data—as well as on Defendant’s role in handling Personal Information, to ensure that their Personal Information would be kept confidential, securely maintained, and disclosed only as authorized.

40. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonably cybersecurity safeguards or policies to protect Plaintiffs’ and Class members’ Personal Information nor adequately trained or supervised its agents and employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients and employees’ Personal Information.

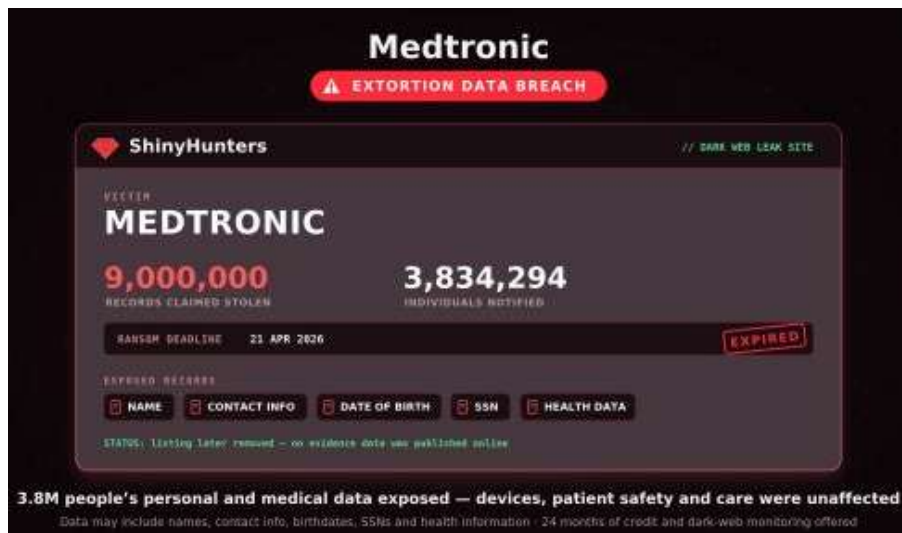
⁷ *Id.*

B. The Data Breach and Defendant's Notice

41. On April 17, 2026, the notorious ransomware gang “ShinyHunters” listed Defendant on its leak website and, on information and belief, posted samples of the information it had stolen from Defendant’s IT Network, including Plaintiffs’ and Class members’ Personal Information, on its dark web leak website.



42. In this post, ShinyHunters issued a final warning to Defendant, stating that Defendant had until April 21, 2026, to pay its ransom or it would leak all 9 million records’ worth of stolen information, including Plaintiffs’ and Class members’ Personal Information, for any and all unauthorized individuals to further access and distribute on the dark web.



43. ShinyHunters is one of the most active ransomware actors, and Defendant, a self-proclaimed leader in its industry, knew or should have known of the tactics that groups like ShinyHunters employ.⁸

⁸ See, e.g., Lawrence Abrams, *Wynn Resorts confirms employee data breach after extortion threat*, BLEEPINGCOMPUTER (Feb. 24, 2026),

44. Ransomware groups like ShinyHunters regularly monetize stolen Personal Information and sell it on the dark web as part of a full identity profile.⁹ Buyers can then use that information to conduct different types of identity theft or fraud, such as filing a fake tax return, applying for a fraudulent mortgage or opening a bank account while impersonating the victim.¹⁰

45. And as the Harvard Business Review notes, such “[c]ybercriminals frequently use the dark web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking.”¹¹

46. To date, Defendant has provided no public information on a ransom demand or payment.

47. On or around April 21, 2026, the same day as the deadline set by ShinyHunters for Defendant to pay its ransom demand and avoid the further disclosure of the Personal Information it stole, Defendant publicly confirmed it experienced a Data Breach and indicated that its investigation into its nature and scope was ongoing.¹² However, it was not until approximately July 1, 2026, that Defendant began issuing formal notice to those impacted by the Data Breach.

48. On information and belief, notice is ongoing, with many Data Breach victims still

<https://www.bleepingcomputer.com/news/security/wynn-resorts-confirms-employee-data-breach-after-extortion-threat/> (last accessed July 22, 2026).

⁹ Anthony M. Freed, *Which Data Do Ransomware Attackers Target for Double Extortion?*, CYBEREASON (Nov. 23, 2021), <https://www.cybereason.com/blog/which-data-do-ransomware-attackers-target-for-double-extortion> (last accessed July 22, 2026).

¹⁰ *Id.*

¹¹ Brenda R. Sharton, *Your Company’s Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back> (last accessed July 22, 2026).

¹² Alessandro Mascellino, *Medtronic Confirms Data Breach After ShinyHunters Claims*, INFOSECURITY MAGAZINE (Apr. 28, 2026), <https://www.infosecurity-magazine.com/news/medtronic-data-breach-shinyhunters/> (last accessed July 22, 2026).

awaiting their formal notice.

49. Defendant delayed notifying victims of the Data Breach despite ShinyHunters publicizing the Data Breach and, on information and belief, sharing the stolen information, including Plaintiffs' and Class members' Personal Information, on the dark web on or around April 21, 2026, almost three months prior.

50. In its Breach Notice, Defendant states: "On April 15, 2026, Medtronic became aware of unusual activity on certain corporate IT systems. Medtronic launched an investigation with the assistance of leading third-party cybersecurity experts to determine the impact and scope of the incident. The investigation determined that from April 13 to April 19, 2026, an unauthorized actor accessed certain Medtronic corporate IT systems." Ex. A.

51. In short, Defendant's cybersecurity practices were so inadequate that not only was the unauthorized bad actor, including at least the notorious cybercriminal gang ShinyHunters, able to access Plaintiffs' and Class members' most sensitive information for almost an entire week; but it was also able to *acquire* and successfully *remove* this information, all without alerting Defendant.

52. The Breach Notice further confirms that the Data Breach impacted "patient[s] with a Medtronic medical device" and that the following types of Personal Information were impacted: "name, contact information, date of birth, Social Security number, and health-related information." Ex. A.

53. Plaintiffs' and Class members' Personal Information is now permanently in the hands of unauthorized bad actors for further dissemination and exploitation. Indeed, this is the *modus operandi* of ShinyHunters and similar cybercriminals.

54. Through its inadequate security practices, Defendant exposed Plaintiffs' and Class members' Personal Information for theft and sale on the dark web.

55. Defendant's delay in notifying Plaintiffs and Class members of the Data Breach exposed them to a longer window of unmitigated risk, during which their Personal Information was in the hands of unauthorized actors and they had no opportunity to take protective measures. In other words, Defendant intentionally kept Plaintiffs and Class members uninformed despite knowing that cybercriminals had accessed Plaintiffs' and Class members' Personal Information as early as April 2026—thereby depriving them of the opportunity to mitigate their injuries in a timely manner.

56. Defendant's Breach Notice acknowledged the significant threat posed by the Data Breach, warning victims "to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors." Ex. A. Defendant further warns that, as a result of the Data Breach, Plaintiffs and Class members must "be cautious of unexpected communications, including emails, text messages or phone calls, requesting personal information." Ex. A.

57. Defendant's Breach Notice also acknowledged its duty to protect patients and employees' Personal Information, insisting that, despite the Data Breach showing otherwise, "[d]ata privacy and security are a top priority for Medtronic" and that Defendant "regret[s]" the impact the Data Breach will have on Plaintiffs and Class members. Ex. A.

58. However, omitted from Defendant's Breach Notice were details of the root cause of the Data Breach, the vulnerabilities exploited, the fact that the notorious cybercriminal ShinyHunters was behind the Data Breach, and the specific remedial measures undertaken to ensure such a breach does not occur again. Indeed, to date, these critical facts have not been explained or clarified to Plaintiffs and Class members, who retain a vested interest in ensuring that their Personal Information remains protected.

59. Instead, Defendant has released only vague statements that "an unauthorized actor

gained access to certain Medtronic corporate IT systems” and that “Medtronic has implemented additional safeguards and continues to work with third-party cybersecurity experts to identify opportunities to further strengthen the security of its systems.” Ex. A.

60. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class members of the Data Breach’s critical facts. Without these details, Plaintiffs’ and Class members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

61. Moreover, Defendant has done little to mitigate the effects of the Data Breach for victims, merely offering certain victims two years of credit monitoring services—a remedy wholly insufficient to compensate Plaintiffs and Class members for the injuries sustained as a result of the Data Breach. Ex. A.

62. Upon information and belief, cybercriminals have and will continue to misuse the Personal Information exfiltrated in the Data Breach, including marketing and selling such Personal Information on the dark web.

63. Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiffs’ and Class members’ Personal Information confidential and to protect such Personal Information from unauthorized access.

64. Nevertheless, Defendant failed to make sufficient efforts to prevent external access, detect outside infiltration, and train its employees to identify cybersecurity threats and defend against them.

65. The stolen Personal Information at issue has great value to the hackers and others due to the large number of individuals affected and sensitivity of the information that was compromised.

66. Defendant breached its obligations and duties to Plaintiffs and Class members

and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Upon information and belief, Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect Plaintiffs' and Class members' Personal Information;
- c. Failing to detect or properly monitor its computer systems for unauthorized intrusions into its computer systems and networks;
- d. Failing to adequately segment its systems and networks so that unauthorized entrants could not traverse in and out of the areas containing Personal Information undetected;
- e. Failing to detect the exfiltration of the most sensitive information (Plaintiffs' and Class members' Personal Information) in its possession;
- f. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- g. Failing to train its employees in the proper handling of Personal Information and maintaining adequate security practices;
- h. Failing to comply with Federal Trade Commission (FTC) guidelines for cybersecurity, in violation of Section 5 of the FTC Act (FTC Act);
- i. Failing to adhere to industry standards for cybersecurity as discussed above; and
- j. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class members' sensitive Personal Information.

67. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class members' Personal Information by allowing cybercriminals to access its computer network and systems which contained unsecured and unencrypted Personal Information.

68. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

C. Common Injuries and Damages

69. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Personal Information ending up in the possession of cybercriminals, the risk of identity theft to Plaintiffs and Class members has materialized and is imminent, and Plaintiffs and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) the loss of benefit of the bargain (price premium damages); (d) negative impact to the value of their Personal Information; and (e) the continued risk to their Personal Information, which remains in the possession of Defendant and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

a. The Data Breach Increases Victims' Risk of Identity Theft

70. Due to the Data Breach, Plaintiffs and Class members are at an indefinite, heightened risk of identity theft.

71. The Personal Information of Class members will be sold on the dark web (to the extent that it has not already been sold) because that is the *modus operandi* of cybercriminals. Indeed, on information and belief, the cybercriminal gang ShinyHunters has already done exactly that. In addition, unencrypted Personal Information is likely to fall into the hands of companies

that will use it for targeted marketing without the approval of Plaintiffs and Class members.

72. The link between data breaches and identity theft risks is simple and well established. Cybercriminals steal Personal Information to sell it on the black market to other criminals who then utilize the information to commit a variety of identity theft-related crimes as discussed below.

73. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on and use the victim's identity or track the victim to decipher passwords or attempt other hacking crimes.

74. 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 log-in 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 can be the starting point for these additional targeted attacks on the victim.

75. One such example of criminals piecing together bits and pieces of compromised Personal Information for profit is the development of "Fullz" packages.¹³

¹³ "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made from those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground*

76. With “Fullz” packages, cybercriminals can cross-reference two sources of Personal Information 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.

77. The development of “Fullz” packages means that the stolen Personal Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class members’ phone numbers, email addresses, driver’s license numbers, 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 Personal Information that was exfiltrated in the Data Breach, criminals may still easily use the Personal Information to create a Fullz package at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

78. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that approximately 39% of victims of identity theft needed a month or more to resolve issues it creates.¹⁴

79. It is within this context that Plaintiffs and Class members must now live with the knowledge that their Personal Information is forever in cyberspace and was taken by individuals intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black market.

ii. Loss of Time to Mitigate Risk of Identity Theft and Fraud

Stolen from Texas Life Insurance Firm, KREBSONSECURITY (Sept. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm> (last accessed July 22, 2026).

¹⁴ *2025 Consumer Impact Report*, IDENTITY THEFT RES. CTR. 27 (Oct. 2025), <https://www.idtheftcenter.org/wp-content/uploads/2025/10/The-2025-ITRC-Consumer-Impact-Report.pdf> (last accessed July 22, 2026).

80. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Personal Information was compromised, the reasonable person is expected to take steps to learn about the breach, address the dangerous situation, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend the time to review accounts and credit reports and take other measures could expose the individual to greater financial harm; but the resource and asset of time is lost where, as here, the company that failed to safeguard the Personal Information also delayed notifying affected individuals.

81. Plaintiffs and Class members have and will continue to spend time on a variety of prudent actions to remedy the harms they have suffered and mitigate those that are likely to occur as a result 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.

82. These efforts are consistent with the U.S. Government Accountability Office which released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”¹⁵

83. These efforts are also consistent with the steps the FTC recommends data breach victims take, which is to protect their personal and financial information by contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to

¹⁵ See *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), <https://www.gao.gov/products/gao-07-737> (last accessed July 22, 2026).

remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.¹⁶

iii. Value of Personal Information

84. Personal Information is a valuable property right, and there is an active and robust legitimate marketplace for Personal Information. Its value is axiomatic, considering the value of “Big Data” in corporate America and the fact that consequences of cyberthefts include heavy prison sentences. The fact that many cybercriminals conclude that the risk of these consequences are outweighed by the potential reward illustrates beyond a doubt that Personal Information has considerable market value.

85. Even in 2019, the data brokering industry was worth roughly \$200 billion.¹⁷ The industry has grown exponentially since then.

86. In fact, 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.¹⁸

87. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$60.00 per year.¹⁹

88. As a result of the Data Breach, the value of Plaintiffs’ and Class members’ Personal Information has been damaged and diminished. This transfer of value occurred without any consideration paid to Plaintiffs or Class members for their property, resulting in an economic loss.

¹⁶ *What To Do Right Away*, FED. TRADE COMM’N, <https://www.identitytheft.gov/Steps> (last accessed July 9, 2026).

¹⁷ David Lazarus, *Shadowy Data Brokers Make the Most of Their Cloak*, L.A. TIMES (Nov. 5, 2019), <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last accessed July 22, 2026).

¹⁸ DATACOU, <https://datacoup.com/> (last accessed July 9, 2026).

¹⁹ *See Frequently Asked Questions*, NIELSEN COMP. & MOBILE PANEL, <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last accessed July 9, 2026).

Moreover, because their Personal Information is now readily available, the rarity of such Personal Information has been lost, thereby causing additional loss of value.

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

89. Given the type of targeted attack in this case, the type of Personal Information involved, and the likely volume of data compromised in the Data Breach, entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchased by criminals intending to utilize the Personal Information for identity-theft-related crimes, such as opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

90. Such fraud may go undetected until debt collection calls commence months, or even years later. For example, an individual may not know that their 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.

91. Consequently, Plaintiffs and Class members are at a present and continuous risk of fraud and identity theft and will need to expend time and resources on credit and identity-theft monitoring for many years into the future.

92. The retail cost of credit and identity theft monitoring can be around \$200 per year. As a result of the Data Breach, this is a reasonable and necessary expense for Plaintiffs and Class members to make in order to monitor and protect themselves from the risk of identity theft. This is a future cost, for a minimum of five years, that Plaintiffs and Class members would not need to bear but for Defendant's failure to safeguard their Personal Information.

v. Lost Benefit of the Bargain

93. Defendant's poor data security deprived Plaintiffs and Class members of the

benefit of their bargain.

94. When agreeing to provide their Personal Information, which was a condition precedent to receiving products, services, and/or employment from Defendant, Plaintiffs and Class members understood and expected that they were, in part, paying for products or services or receiving lesser wages or employment conditions in exchange for data security to protect the Personal Information they were required to provide.

95. Plaintiffs value data security. Indeed, data security is an important consideration when seeking products, services, and employment.

96. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year Consumer Privacy Survey.²⁰ Cisco reported the following: “Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly.”²¹ Of the consumers surveyed, 89% stated that “I care about data privacy.”²² 83% of consumers declared that they are “willing to spend time and money to protect data” and that they “expect to pay more” for privacy.²³

97. Defendant did not provide the bargained-for and expected data security. Accordingly, Plaintiffs and Class members received products, services, and employment conditions of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

²⁰ *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO (2024), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last accessed July 22, 2026).

²¹ *Id.*

²² *Id.* at 9.

²³ *Id.*

D. Defendant Failed to Comply with HIPAA Guidelines

98. Defendant is a covered entity under the Health Insurance Portability and Accountability Act (“HIPAA”) (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Parts 160 Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule 45 C.F.R. Parts 160 Part 164, Subparts A and C (“Security Standards for the Protection of Electronic Protected Health Information”).

99. Defendant is also subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).²⁴ *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

100. HIPAA’s Privacy Rule establishes national standards for the protection of health information.

101. HIPAA’s Security Rule establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

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

103. “Electronic protected health information” is “individually identifiable health information . . . that is (i) [t]ransmitted by electronic media; (ii) [m]aintained in electronic media; or (iii) [t]ransmitted or maintained in any other form or medium.” 45 C.F.R. § 160.103.

104. HIPAA’s Security Rule requires Defendant to:

a. Ensure the confidentiality, integrity, and availability of all electronic

²⁴ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

protected health information the covered entity or business associate creates, receives, maintains, or transmits;

- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by its workforce.

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

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

107. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of a data breach to each affected individual “without unreasonable delay and in no case later than 60 days following discovery of the breach.”²⁵

²⁵ *Breach Notification Rule*, U.S. DEP’T OF HEALTH & HUMAN SERVICES, <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (last accessed July 9, 2026).

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

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

110. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of [electronic protected health information] and comply with the risk analysis requirements of the Security Rule.”²⁶ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing [electronic protected health information].”²⁷

²⁶ *Security Rule Guidance Material*, U.S. DEP’T OF HEALTH & HUMAN SERVICES, <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html> (last accessed July 9, 2026).

²⁷ *Guidance on Risk Analysis*, U.S. DEP’T OF HEALTH & HUMAN SERVICES, <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> (last accessed July 9, 2026).

E. Defendant as on Notice of Cyber Attack Threats and of the Inadequacy of Its Data Security

111. Data security breaches have dominated the headlines for the last two decades. The general public is broadly aware of some of the largest cybersecurity breaches, including against major healthcare companies like Defendant: United HealthGroup, Target,²⁸ Yahoo,²⁹ Marriott International,³⁰ Chipotle, Chili's, Arby's,³¹ among others.³²

112. Defendant knew or should have known that it was at risk of a data breach that could expose the Personal Information that it collected and maintained.

113. Defendant was also on notice of the importance of data encryption for Personal Information. Defendant knew it maintained Personal Information in its systems yet seemingly did not encrypt these systems or the information contained within them.

F. Cyber Criminals Will Use Plaintiffs and Class Members' Personal Information to Commit Fraud

114. Plaintiffs and Class members' Personal Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been and will continue to be used

²⁸ Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/> (last accessed July 22, 2026).

²⁹ Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), <https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html> (last accessed July 22, 2026).

³⁰ Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE (Mar. 22, 2019), <https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/> (last accessed July 22, 2026).

³¹ Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), <https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b> (last accessed July 22, 2026).

³² See, e.g., Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html> (last accessed July 22, 2026).

in a variety of sordid ways to exploit Plaintiffs and Class members and to profit off their misfortune.

115. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.³³ For example, with the Personal Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.³⁴ These criminal activities have and will continue to result in devastating financial and personal losses to Plaintiffs and Class members.

116. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.³⁵

117. Based on the foregoing, the Personal Information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because there, victims can cancel or close credit and debit card accounts. The Personal Information compromised in this Data Breach, including names and Social Security numbers, is impossible to "close" and difficult, if not impossible, to change.

³³ *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (last accessed July 9, 2026) (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

³⁴ John Egan, *What should I do if My Driver's License Number Is Stolen?*, EXPERIAN (June 13, 2024), <https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/> (last accessed July 22, 2026).

³⁵ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), <https://www.gao.gov/products/gao-07-737> (last accessed July 22, 2026).

118. This data demands a significantly higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”³⁶

119. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit from the ransom and sale of Plaintiffs’ and Class members’ Personal Information on the dark web. The Personal Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

120. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.³⁷

121. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[I]n 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.³⁸

122. As described above, identity theft victims must spend countless hours and large

³⁶ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, NETWORK WORLD, (Feb. 6, 2015), <https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed July 22, 2026).

³⁷ Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARYCONSUMER (May 24, 2017), <https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info> (last accessed July 22, 2026).

³⁸ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), <https://www.gao.gov/products/gao-07-737> (last accessed July 22, 2026).

amounts of money repairing the impact to their credit.³⁹

123. With the Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

124. Victims of the Data Breach, like Plaintiffs and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.⁴⁰

125. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and Class members have suffered, and have been placed at an imminent and continuing increased risk of suffering harm from fraud and identity theft. Plaintiffs and Class members must now expend the time, effort, and money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services; placing freezes and alerts with credit reporting agencies; contacting financial institutions and healthcare providers; closing or modifying financial accounts; and closely monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

126. Plaintiffs and Class members have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

- a. Trespass, damage to, and theft of their personal property including their Personal Information;
- b. Improper disclosure of their Personal Information;
- c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the

³⁹ *Guide for Assisting Identity Theft Victims*, FTC 4 (Sept. 2013), <https://www.hiresafe.com/wp-content/uploads/2019/10/Guide-for-Assisting-ID-Theft-Victims.pdf> (last accessed July 22, 2026).

⁴⁰ *Id.*

- hands of criminals;
- d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;
- e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;
- f. Loss of privacy suffered as a result of the Data Breach;
- g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;
- h. Ascertainable losses in the form of deprivation of the value of their Personal Information;
- i. The loss of use of and access to their credit, accounts, and/or funds;
- j. Damage to their credit due to fraudulent use of their Personal Information; and
- k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

127. Moreover, Plaintiffs and Class members have an interest in ensuring that their Personal Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiffs' and Class members' Personal Information.

128. Plaintiffs and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the Personal Information Defendant made accessible to hackers, they are certain to incur additional damages. Because cybercriminals have their Personal

Information, Plaintiffs and Class members will need to have identity theft monitoring protection for the rest of their lives.

G. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' Personal Information

129. Data breaches are preventable.⁴¹ As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, “[i]n 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.”⁴² She added that “[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised.”⁴³

130. “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*.”⁴⁴

131. The 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.

132. 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

⁴¹ Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

⁴²*Id.* at 17.

⁴³*Id.* at 28.

⁴⁴*Id.*

dispose of Personal Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. 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.⁴⁵

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

134. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

135. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in

⁴⁵ *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed July 6, 2026).

violation of Section 5 of the FTC Act.”).

136. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

137. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to customers’ Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

138. Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

139. Defendant was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of Plaintiffs’ and Class members’ Personal Information.

140. Many failures laid the groundwork for the Data Breach, starting with Defendant’s failure to incur the costs necessary to implement adequate and reasonable cybersecurity procedures and protocols to protect Plaintiffs’ and Class members’ Personal Information.

141. Defendant was at all times fully aware of its obligation to protect the Personal Information of Plaintiffs and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

142. Defendant maintained the Personal Information in a reckless manner. In particular, the Personal Information was maintained and/or exchanged, unencrypted, in Defendant’s systems and was maintained in a condition vulnerable to cyberattacks.

143. Defendant knew, or reasonably should have known, of the importance of

safeguarding Personal Information and of the foreseeable consequences that would occur if it failed to do so, including the significant costs that would be placed on Plaintiffs and Class members as a result of a breach.

144. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class members' Personal Information from those risks left that information in a dangerous condition.

145. Defendant disregarded the rights of Plaintiffs and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' Personal Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

H. Plaintiffs' Experiences and Injuries

Plaintiff Rath

146. Plaintiff Rath is a consumer and a victim of the Data Breach. As a condition of receiving the medical devices and/or services from Defendant, Plaintiff Rath provided Defendant (or third-party agents) with his Personal Information.

147. Plaintiff Rath trusted that Defendant would use reasonable measures to protect his Personal Information and that Defendant's cybersecurity measures were in line with industry standards and state and federal law.

148. On information and belief, Plaintiff Rath's Personal Information has already been

published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

149. Defendant deprived Plaintiff Rath of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him of the Data Breach.

150. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Rath's Personal Information to theft by cybercriminals and sale on the dark web.

151. As a result of the Data Breach, Plaintiff Rath suffered actual injury in the form of damages and/or negative impact to the value of his Personal Information, among other damages.

152. Plaintiff Rath has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing online account passwords, placing a credit freeze through all three main credit bureaus, and monitoring his credit information.

153. Plaintiff Rath fears for his personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Rath has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

154. Indeed, following the Data Breach, Plaintiff Rath was alerted to fraudulent charges on his credit card that, on information and belief, Defendant possessed and that was likely stolen in the Data Breach. Plaintiff Rath did not recognize and certainly did not authorize or recognize these charges.

155. Plaintiff Rath was forced to spend time and effort communicating with his credit card company in order to resolve these fraudulent charges.

156. On information and belief, the fraudulent charges that Plaintiff Rath is experiencing are a result of the Data Breach. Indeed, the information exposed by Defendant's Data Breach was more than enough for cybercriminals to use and gather additional information

to compromise his credit card.

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

Plaintiff Corvia

158. Plaintiff Corvia is an employee of Defendant and, on information and belief, a victim of the Data Breach. As a condition of receiving employment and payroll services from Defendant, Plaintiff Corvia provided Defendant her Personal Information.

159. Plaintiff Corvia trusted that Defendant would use reasonable measures to protect her Personal Information and that Defendant's cybersecurity measures were in line with industry standards and state and federal law.

160. On information and belief, Plaintiff Corvia's Personal Information has already been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

161. Defendant deprived Plaintiff Corvia of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her of the Data Breach.

162. On or around March 25, 2026, Plaintiff Corvia received an internal email from Defendant advising employees to avoid suspicious emails. Defendant's systems went down on or around April 15, 2026. On April 29, 2026, Defendant informed Plaintiff Corvia that there was a possible data breach and advised her to obtain Credit Karma.

163. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Corvia's Personal Information to theft by cybercriminals and sale on the dark web.

164. As a result of the Data Breach, Plaintiff Corvia suffered actual injury in the form of damages and negative impact to the value of her Personal Information, among other damages.

165. Plaintiff Corvia has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through all three main credit bureaus, and monitoring her credit information.

166. Plaintiff Corvia fears for her personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Corvia has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

167. Shortly following the Data Breach, Plaintiff Corvia began receiving a substantial influx of spam phone calls and texts. On information and belief, these spam calls and texts are on the same phone number that Defendant retains in relation to Plaintiff Corvia and that were exposed during the Data Breach.

168. Also following the Data Breach, Plaintiff Corvia began receiving unsolicited and suspicious Facebook friend requests to her personal Facebook account, which is linked to the same personal email account and phone number that, on information and belief, Defendant possessed and that were likely stolen in the Data Breach.

169. On information and belief, the suspicious Facebook requests, as well as the spam calls and texts that Plaintiff Corvia is experiencing are results of the Data Breach. Indeed, the information exposed by Defendant's Data Breach was more than enough for cybercriminals to use and gather additional information to send her spam texts and calls as well as send her suspicious Facebook requests.

170. Plaintiff Corvia has a continuing interest in ensuring her Personal Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Jennings

171. Plaintiff Jennings is a consumer and a victim of the Data Breach. As a condition of receiving medical devices and/or services from Defendant, Plaintiff Jennings provided Defendant (or third-party agents) with her Personal Information.

172. Plaintiff Jennings trusted that Defendant would use reasonable measures to protect her Personal Information and that Defendant's cybersecurity measures were in line with industry standards and according to state and federal law.

173. On information and belief, Plaintiff Jennings' Personal Information has already been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

174. Defendant deprived Plaintiff Jennings of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her of the Data Breach.

175. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Jennings' Personal Information to theft by cybercriminals and sale on the dark web.

176. As a result of the Data Breach, Plaintiff Jennings suffered actual injury in the form of damages and negative impact to the value of her Personal Information, among other damages.

177. Plaintiff Jennings has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through all three main credit bureaus, and monitoring her credit information.

178. Plaintiff Jennings fears for her personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Jennings has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

179. Shortly following the Data Breach, Plaintiff Jennings began receiving a substantial

influx of spam phone calls and texts. On information and belief, these spam calls and texts are on the same phone number that Defendant retains in relation to Plaintiff Jennings and that was exposed during the Data Breach.

180. Also following the Data Breach, in or around April and May 2026, Plaintiff Jennings was alerted to her Amazon account being hacked and used by an unauthorized individual to make several fraudulent purchases that she did not recognize and certainly did not authorize. On information and belief, her Amazon account utilized the same contact information, including email account, phone number, and home address, that Defendant possessed and, on information and belief, that were likely stolen in the Data Breach.

181. As a result of the fraudulent Amazon purchases, Plaintiff Jennings was forced to spend time and effort securing her Amazon account, including regaining access to her account and cancelling these purchases.

182. On information and belief, the successful hacking of her Amazon account, the fraudulent Amazon purchases, as well as the spam calls and texts that Plaintiff Jennings is experiencing is a result of the Data Breach. Indeed, the information exposed by the Data Breach was more than enough for cybercriminals to use and gather additional information to compromise her Amazon account as well as to send her spam texts and calls.

183. Plaintiff Jennings has a continuing interest in ensuring her Personal Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Loughry

184. Plaintiff Loughry is a consumer and a victim of the Data Breach. As a condition of receiving medical devices and/or services from Defendant, Plaintiff Loughry provided Defendant (or third-party agents) with his Personal Information. Indeed, Defendant required

Plaintiff Loughry to provide that Personal Information to obtain its services and devices.

185. Plaintiff Loughry trusted that Defendant would use reasonable measures to protect his Personal Information and that Defendant's cybersecurity measures were in line with industry standards and state and federal law.

186. On information and belief, Plaintiff Loughry's Personal Information has already been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

187. Defendant deprived Plaintiff Loughry of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him of the Data Breach.

188. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Loughry's Personal Information to theft by cybercriminals and sale on the dark web.

189. As a result of the Data Breach, Plaintiff Loughry suffered actual injury in the form of damages and negative impact to the value of his Personal Information, among other damages.

190. Plaintiff Loughry has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, and monitoring his credit information.

191. Plaintiff Loughry fears for his personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Loughry has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

192. Shortly following the Data Breach, Plaintiff Loughry began receiving a substantial influx of spam phone calls, texts, and emails. On information and belief, these spam calls, texts, and emails are on the same phone number and email address that Defendant retains in relation to

Plaintiff Loughry and that were exposed during the Data Breach.

193. Indeed, the information exposed by the Data Breach was more than enough for cybercriminals to use and gather additional information to send him spam texts, calls, and emails.

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

Plaintiff McLain

195. Plaintiff McLain is a former employee of Defendant and, on information and belief, a victim of the Data Breach. As a condition of receiving employment and payroll services from Defendant, Plaintiff McLain provided Defendant his Personal Information.

196. Plaintiff McLain trusted that Defendant would use reasonable measures to protect his Personal Information and that Defendant's cybersecurity measures were in line with industry standards and state and federal law.

197. On information and belief, Plaintiff McLain's Personal Information has already been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

198. Defendant deprived Plaintiff McLain of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him of the Data Breach.

199. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff McLain's Personal Information to theft by cybercriminals and sale on the dark web.

200. As a result of the Data Breach, Plaintiff McLain suffered actual injury in the form of damages and impact to the value of his Personal Information, among other damages.

201. Plaintiff McLain has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit

card and financial account statements, changing his online account passwords, placing a credit freeze through Experian and TransUnion, and monitoring his credit information.

202. Plaintiff McLain fears for his personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff McLain has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

203. Shortly following the Data Breach, Plaintiff McLain began receiving a substantial influx of spam phone calls and texts. On information and belief, these spam calls and texts are on the same phone number that Defendant retains in relation to Plaintiff McLain and that was exposed during the Data Breach.

204. On information and belief, the suspicious spam calls and texts that Plaintiff McLain is experiencing is a result of the Data Breach. Indeed, the information exposed by the Data Breach was more than enough for cybercriminals to use and gather additional information to send him spam texts and calls.

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

Plaintiff Buckner

206. Plaintiff Buckner is a consumer and a victim of the Data Breach. As a condition of receiving medical devices and/or services from Defendant, Plaintiff Buckner provided Defendant (or third-party agents) with her Personal Information.

207. Plaintiff Buckner trusted that Defendant would use reasonable measures to protect her Personal Information and that Defendant's cybersecurity measures were in line with industry standards and according to state and federal law.

208. On information and belief, Plaintiff Buckner's Personal Information has already

been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

209. Defendant deprived Plaintiff Buckner of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her of the Data Breach.

210. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Buckner's Personal Information to theft by cybercriminals and sale on the dark web.

211. As a result of the Data Breach, Plaintiff Buckner suffered actual injury in the form of damages and negative impact to the value of her Personal Information, among other damages.

212. Plaintiff Buckner has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through all three main credit bureaus, and monitoring her credit information.

213. Plaintiff Buckner fears for her personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Buckner has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

214. Shortly following the Data Breach, Plaintiff Buckner began receiving a substantial influx of spam phone calls and texts. On information and belief, these spam calls and texts are on the same phone number that Defendant retains in relation to Plaintiff Buckner and that was exposed during the Data Breach.

215. Also following the Data Breach, Plaintiff Buckner was alerted by her banks to several unauthorized charges on her bank cards that she did not recognize and certainly did not authorize. On information and belief, these unauthorized charges were on the same accounts that Defendant possessed the financial information of, on information and belief, that were likely

stolen in the Data Breach.

216. Plaintiff Buckner also received alerts from Credit Karma and Experian informing her that her Personal Information had been found on the dark web.

217. On information and belief, the fraudulent charges, as well as the spam calls and texts that Plaintiff Buckner is experiencing is a result of the Data Breach. Indeed, the information exposed by the Data Breach was more than enough for cybercriminals to use and gather additional information to compromise her credit and bank cards as well as to send her spam texts and calls.

218. Plaintiff Buckner has a continuing interest in ensuring her Personal Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Riley

219. Plaintiff Riley is a consumer and, on information and belief, a victim of the Data Breach. As a condition of receiving medical devices and/or services from Defendant, Plaintiff Riley provided Defendant (or third-party agents) with her Personal Information.

220. Plaintiff Riley trusted that Defendant would use reasonable measures to protect her Personal Information and that Defendant's cybersecurity measures were in line with industry standards and according to state and federal law.

221. On information and belief, Plaintiff Riley's Personal Information has already been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

222. Defendant deprived Plaintiff Riley of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her of the Data Breach.

223. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Riley's Personal Information to theft by cybercriminals and sale on the dark web.

224. As a result of the Data Breach, Plaintiff Riley suffered actual injury in the form of damages and negative impact to the value of her Personal Information, among other damages.

225. Plaintiff Riley has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through all three main credit bureaus, and monitoring her credit information.

226. Plaintiff Riley fears for her personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Riley has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

227. On information and belief, the spam calls and emails that Plaintiff Riley is experiencing is a result of the Data Breach. Indeed, the information exposed by the Data Breach was more than enough for cybercriminals to use and gather additional information to send her spam emails and calls.

228. Plaintiff Riley has a continuing interest in ensuring her Personal Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Kennedy

229. Plaintiff Kennedy is a consumer and a victim of the Data Breach. As a condition of receiving medical devices and/or services from Defendant, Plaintiff Kennedy provided Defendant (or third-party agents) with his Personal Information.

230. Plaintiff Kennedy trusted that Defendant would use reasonable measures to protect his Personal Information and that Defendant's cybersecurity measures were in line with industry standards and state and federal law.

231. On information and belief, Plaintiff Kennedy's Personal Information has already

been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

232. Defendant deprived Plaintiff Kennedy of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him of the Data Breach.

233. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Kennedy's Personal Information to theft by cybercriminals and sale on the dark web.

234. As a result of the Data Breach, Plaintiff Kennedy suffered actual injury in the form of damages and negative impact to the value of his Personal Information, among other damages.

235. Plaintiff Kennedy has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, and monitoring his credit information.

236. Plaintiff Kennedy fears for his personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Kennedy has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

237. Following the Data Breach, Plaintiff Kennedy began receiving a substantial influx of spam phone calls, texts, and emails. On information and belief, these spam calls, texts, and emails are on the same phone number and email address that Defendant retains in relation to Plaintiff Kennedy and that were exposed during the Breach.

238. As a result of the Data Breach, Plaintiff Kennedy now receives approximately 6–15 spam calls, 10–15 spam texts, and approximately 20 spam emails per day. The spam callers will occasionally leave a voicemail that amounts to approximately 30 seconds of silence.

239. Plaintiff Kennedy also received an alert from Chase informing him that an

unknown individual was inquiring into his credit.

240. On information and belief, the spam phone calls, texts, and emails, as well as the fraudulent inquiry into his credit that Plaintiff Kennedy is experiencing is a result of the Data Breach. Indeed, the information exposed by the Data Breach was more than enough for cybercriminals to use and gather additional information to send him spam texts, calls, and emails as well as inquire into his credit.

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

Plaintiff Lindley

242. Plaintiff Lindley is a consumer and a victim of the Data Breach. As a condition of receiving medical devices and/or services from Defendant, Plaintiff Lindley provided Defendant (or third-party agents) with her Personal Information.

243. Plaintiff Lindley trusted that Defendant would use reasonable measures to protect her Personal Information and that Defendant's cybersecurity measures were in line with industry standards and according to state and federal law.

244. On information and belief, Plaintiff Lindley's Personal Information has already been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

245. Defendant deprived Plaintiff Lindley of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her of the Data Breach.

246. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Lindley's Personal Information to theft by cybercriminals and sale on the dark web.

247. As a result of the Data Breach, Plaintiff Lindley suffered actual injury in the form

of damages and negative impact to the value of her Personal Information, among other damages.

248. Plaintiff Lindley has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through all three main credit bureaus, and monitoring her credit information.

249. Plaintiff Lindley fears for her personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Lindley has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

250. Following the Data Breach, Plaintiff Lindley began receiving a substantial influx of spam phone calls and texts. On information and belief, these spam calls and texts are on the same phone number that Defendant retains in relation to Plaintiff Lindley and that was exposed during the Breach.

251. As a result of the Data Breach, Plaintiff Lindley now receives approximately 25 spam calls, 50 spam emails, and 50 spam texts per day. These spam calls, emails, and texts often involve the attempted sale of various products as well as cleaning services.

252. Plaintiff Lindley also received an alert from Experian informing her that her sensitive information had been found on the dark web.

253. On information and belief, the spam calls and texts that Plaintiff Lindley is experiencing is a result of the Data Breach. Indeed, the information exposed by the Data Breach was more than enough for cybercriminals to use and gather additional information to send her spam calls and texts.

254. Plaintiff Lindley has a continuing interest in ensuring her Personal Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Spano

255. Plaintiff Spano is a consumer and a victim of the Data Breach. As a condition of receiving medical devices and/or services from Defendant, Plaintiff Spano provided Defendant (or third-party agents) with his Personal Information. Indeed, Defendant required Plaintiff Spano to provide that Personal Information to obtain its services and devices.

256. Plaintiff Spano trusted that Defendant would use reasonable measures to protect his Personal Information and that Defendant's cybersecurity measures were in line with industry standards and state and federal law.

257. On information and belief, Plaintiff Spano's Personal Information has already been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

258. Defendant deprived Plaintiff Spano of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him of the Data Breach.

259. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Spano's Personal Information to theft by cybercriminals and sale on the dark web.

260. As a result of the Data Breach, Plaintiff Spano suffered actual injury in the form of damages and negative impact to the value of his Personal Information, among other damages.

261. Plaintiff Spano has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through all three main credit bureaus, and monitoring his credit information.

262. Plaintiff Spano fears for his personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Spano has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

263. Shortly following the Data Breach, on or around May 2026, Plaintiff Spano was alerted to a fraudulent charge from Walmart, totalling approximately \$106. Plaintiff Spano did not recognize and certainly did not authorize this charge.

264. Plaintiff Spano was forced to spend time and effort communicating with his bank in order to resolve this fraudulent charge.

265. Plaintiff Spano also received an alert informing him that his sensitive information had been found on the dark web.

266. The information exposed by Data Breach was more than enough for cybercriminals to use and gather additional information to cause the fraudulent charge on his bank account.

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

Plaintiff Holmes

268. Plaintiff Holmes is a consumer and a victim of the Data Breach. As a condition of receiving medical devices and/or services from Defendant, Plaintiff Holmes provided Defendant (or third-party agents) with his Personal Information. Indeed, Defendant required Plaintiff Holmes to provide that Personal Information to obtain its services and devices.

269. Plaintiff Holmes trusted that Defendant would use reasonable measures to protect his Personal Information and that Defendant's cybersecurity measures were in line with industry standards and state and federal law.

270. On information and belief, Plaintiff Holmes' Personal Information has already been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

271. Defendant deprived Plaintiff Holmes of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him of the Data Breach.

272. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Holmes' Personal Information to theft by cybercriminals and sale on the dark web.

273. As a result of the Data Breach, Plaintiff Holmes suffered actual injury in the form of damages and negative impact to the value of his Personal Information, among other damages.

274. Plaintiff Holmes has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through all three main credit bureaus, and monitoring his credit information.

275. Plaintiff Holmes fears for his personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Holmes has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

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

Plaintiff Egbert

277. Plaintiff Egbert is a consumer and a victim of the Data Breach. As a condition of receiving medical devices and/or services from Defendant, Plaintiff Egbert provided Defendant (or third-party agents) with her Personal Information. Indeed, Defendant required Plaintiff Egbert to provide that Personal Information to obtain its services and devices.

278. Plaintiff Egbert trusted that Defendant would use reasonable measures to protect her Personal Information and that Defendant's cybersecurity measures were in line with industry standards and state and federal law.

279. On information and belief, Plaintiff Egbert's Personal Information has already been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

280. Defendant deprived Plaintiff Egbert of the earliest opportunity to guard herself against the Data Breach's effects by failing to promptly notify her of the Data Breach.

281. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Egbert's Personal Information to theft by cybercriminals and sale on the dark web.

282. As a result of the Data Breach, Plaintiff Egbert suffered actual injury in the form of damages and negative impact to the value of her Personal Information, among other damages.

283. Plaintiff Egbert has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit information.

284. Plaintiff Egbert fears for her personal financial security and uncertainty over what Personal Information was exposed in the Data Breach. Plaintiff Egbert has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach.

285. Plaintiff Egbert has a continuing interest in ensuring her Personal Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

I. Defendant Had an Obligation to Protect Personal Information Under the Law and the Applicable Standard of Care

286. Defendant is prohibited by the FTC Act (15 U.S.C. § 45) 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 personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

287. Defendant is further required by various states' laws and regulations to protect Plaintiffs' and Class members' Personal Information.

288. Defendant owed a duty to Plaintiffs and Class members to design, maintain, and test its computer and application systems to ensure that the Personal Information in its possession was adequately secured and protected.

289. Defendant owed a duty to Plaintiffs and Class members to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees (and others who had access to Personal Information within its computer systems) on how to adequately protect Personal Information.

290. Defendant owed a duty to Plaintiffs and Class members to implement processes that would detect a breach of its systems in a timely manner.

291. Defendant owed a duty to Plaintiffs and Class members to act upon data security warnings and alerts in a timely fashion.

292. Defendant owed a duty to Plaintiffs and Class members to disclose that its computer systems and data security practices were inadequate to safeguard individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to entrust such Personal Information to Defendant.

293. Defendant owed a duty to Plaintiffs and Class members to disclose in a timely and accurate manner when data breaches occurred.

294. Defendant owed a duty of care to Plaintiffs and Class members because it was a foreseeable target of a data breach.

V. CLASS ACTION ALLEGATIONS

295. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

296. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of the Classes, defined as follows (and together referred to herein as the “Class”):

Nationwide Class: All persons residing in the United States whose Personal Information was compromised in the Data Breach.

California Subclass: All persons residing in the State of California whose Personal Information was compromised in the Data Breach.

297. Plaintiffs reserve the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

298. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

299. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable.

300. **Typicality:** Plaintiffs’ claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendant’s uniform misconduct. The same event and conduct that gave rise to Plaintiffs’ claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive Personal Information compromised in the same way as a result of the same conduct of Defendant.

301. **Adequacy:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs’ counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

302. **Superiority:** A class action is superior to other available means of adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is

relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system, given the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

303. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

- a. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's Personal Information;
- b. Whether Defendant's email and computer systems and data security practices used to protect Plaintiffs' and Class members' Personal Information violated the FTC Act, state laws, and/or other duties discussed herein;
- c. Whether Defendant owed a duty to Plaintiffs and Class members to adequately protect their Personal Information, and whether it breached that duty;
- d. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to

- a data breach;
- e. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach and Plaintiffs' and Class members' injuries;
- f. Whether Defendant breached contractual duties owed to Plaintiffs and Class members to use reasonable care in protecting their Personal Information;
- g. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals without unreasonable delay, and whether this caused damages to Plaintiffs and Class members;
- h. Whether Defendant continues to breach its duties to Plaintiffs and Class members;
- i. Whether Plaintiffs and Class members suffered injuries as a proximate result of Defendant's negligent actions or failures to act;
- j. Whether Plaintiffs and Class members are entitled to recover damages, equitable relief, and other relief;
- k. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs, Class members, and the general public;
- l. Whether Defendant's actions alleged herein constitute gross negligence; and
- m. Whether Plaintiffs and Class members are entitled to punitive damages.

VI. CAUSES OF ACTION

COUNT ONE **NEGLIGENCE**

(On Behalf of Plaintiffs and the Nationwide Class)

304. Plaintiffs reallege all previous paragraphs as if fully set forth herein.

305. Defendant solicited, gathered, and stored the Personal Information of Plaintiffs and Class members as part of the operation of its business.

306. Upon accepting and storing the Personal Information of Plaintiffs and Class members, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

307. Defendant had full knowledge of the sensitivity of the Personal Information, the types of harm that Plaintiffs and Class members could and would suffer if the Personal Information was wrongfully disclosed, and the importance of adequate security.

308. Plaintiffs and Class members were the foreseeable victims of the inadequate safety and security practices on the part of Defendant. Plaintiffs and Class members had no ability to protect their Personal Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and Class members.

309. Defendant knew that cyber criminals routinely target large corporations through cyberattacks to steal sensitive Personal Information.

310. Defendant owed Plaintiffs and Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and Class members when obtaining, storing, using, and managing Personal Information, including taking action to reasonably safeguard such data and notifying Plaintiffs and Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

311. Defendant's duty extended to protecting Plaintiffs and Class members 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.

312. Defendant had duties to protect and safeguard the Personal Information of Plaintiffs and Class members from cyberattacks by taking common-sense precautions when dealing with sensitive Personal Information. Duties that Defendant owed Plaintiffs and Class members include:

- a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, email accounts, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' Personal Information was adequately secured from impermissible release, disclosure, and publication;
- b. To protect Plaintiffs' and Class members' Personal Information in its possession by using reasonable and adequate security procedures and systems;
- c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its business email system, networks and servers; and
- d. To promptly notify Plaintiffs and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

313. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Personal Information that Plaintiffs and Class members had entrusted to it.

314. Defendant breached its duty of care by failing to adequately protect Plaintiffs' and Class members' Personal Information. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Personal Information in its possession;
- b. Failing to protect the Personal Information in its possession by using reasonable and adequate security procedures and systems;
- c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;
- d. Failing to use adequate email security systems, including healthcare industry standard SPAM filters, DMARC enforcement, and/or sender policy framework enforcement to protect against phishing emails;
- e. Failing to adequately and properly audit, test, and train its employees on how to properly and securely transmit and store Personal Information;
- f. Failing to adequately train its employees to not store Personal Information longer than absolutely necessary for the specific purpose that it was sent or received;
- g. Failing to consistently enforce security policies aimed at protecting Personal Information;
- h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;
- i. Failing to promptly notify Plaintiffs and Class members of the Data Breach that affected their Personal Information.

315. Defendant's willful failure to abide by these duties was wrongful, reckless, and

grossly negligent in light of the foreseeable risks and known threats.

316. Through Defendant's acts and omissions described herein, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Personal Information of Plaintiffs and Class members while it was within Defendant's possession and control.

317. Further, through its failure to provide timely and detailed notice of the Data Breach to Plaintiffs and Class members, Defendant prevented Plaintiffs and Class members from taking meaningful, proactive steps toward securing their Personal Information and mitigating damages.

318. As a result of the Data Breach, Plaintiffs and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to fraudulent activity, closely monitoring bank account activity, and examining credit reports and statements sent from providers and insurance companies.

319. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

320. The damages Plaintiffs and Class members have suffered and will suffer (as alleged herein) were and are the direct and proximate result of Defendant's grossly negligent conduct.

321. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft, are the types of harm that these statutes and regulations intended to prevent.

322. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiffs and Class members to provide fair and adequate computer systems and data security to safeguard

the Personal Information of Plaintiffs and Class members.

323. The FTC Act prohibits “unfair practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also formed part of the basis of Defendant’s duty in this regard.

324. Defendant gathered and stored the Personal Information of Plaintiffs and Class members as part of its business of soliciting and facilitating its services to its patients and employees, which affect commerce.

325. Defendant violated the FTC Act by failing to use reasonable measures to protect the Personal Information of Plaintiffs and Class members and by not complying with applicable industry standards, as described herein.

326. Defendant breached its duties to Plaintiffs and Class members under the FTC Act by failing to provide reasonable or adequate computer systems and/or data security practices to safeguard Plaintiffs’ and Class members’ Personal Information, and by failing to provide prompt and specific notice without reasonable delay.

327. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

328. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

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

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

331. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

332. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

333. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members have suffered, and continue to suffer, damages arising from the Data Breach.

334. Plaintiffs and Class members have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

COUNT TWO
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

335. Plaintiffs reallege all previous paragraphs as if fully set forth herein.

336. Plaintiffs bring this claim on behalf of the Class and in the alternative to all other claims and remedies at law.

337. Plaintiffs and Class members conferred a benefit on Defendant in the form of

profits to render certain services and/or having wages or employment benefits withheld, a portion of which was intended to have been used by Defendant for data security measures to secure Plaintiffs' and Class members' Personal Information.

338. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant chose to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members suffered as a direct and proximate result of Defendant's failure to provide adequate security.

339. Under the principles of equity and good conscience, Defendant should not be permitted to retain the full value of its revenue or profits resulting from its collection and storage of Plaintiffs' and Class members' Personal Information because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

340. If Plaintiffs and Class members knew that Defendant had not secured their Personal Information, they would not have agreed to disclose such Personal Information to Defendant.

341. Defendant collected, maintained, and stored the Personal Information of Plaintiffs and Class members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it (including the use of valuable Personal Information for business purposes and financial gain).

342. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with the entities that collected Plaintiffs' and Class members' Personal Information, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on reasonable data privacy and security

measures to secure Plaintiffs' and Class members' Personal Information.

343. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Personal Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiffs and Class members.

344. Defendant failed to implement—or adequately implement—data security practices, procedures, and programs to secure sensitive Personal Information, including without limitation those industry standard data security practices, procedures, and programs discussed herein.

345. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiffs and Class members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiffs' and Class members' Personal Information, (ii) time and expenses mitigating harms, (iii) diminished and/or negatively impacted value of Personal Information, (iv) loss of privacy, (v) harms as a result of identity theft; and (vi) an increased risk of future identity theft.

346. Defendant, upon information and belief, has therefore engaged in opportunistic and unethical conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiffs and Class members in direct violation of Plaintiffs' and Class members' interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

347. Accordingly, Plaintiffs and Class members are entitled to relief in the form of

restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiffs and Class members.

COUNT THREE
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

348. Plaintiffs reallege all previous paragraphs as if fully set forth herein.

349. Plaintiffs and Class members were required to provide Defendant with their Personal Information in order to receive medical care, treatment and/or employment services.

350. When Plaintiffs and Class members provided their Personal Information to Defendant, they entered into implied contracts with Defendant.

351. Pursuant to these implied contracts, Plaintiffs and Class members, directly or indirectly, paid money to Defendant and provided Defendant with their Personal Information. In exchange, Defendant agreed to, and Plaintiffs and Class members reasonably understood that Defendant would, *inter alia*: (1) provide services and/or employment to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' Personal Information; and (3) protect Plaintiffs' and Class members' Personal Information in compliance with federal and state laws, regulations, and industry standards.

352. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and Class members' Personal Information, Defendant had an implied duty to safeguard their Personal Information. Upon information and belief, this implied duty was reinforced by Defendant's representations in its privacy policy.

353. The protection of Personal Information was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Defendant, on the other hand. Had Plaintiffs and Class members known that Defendant would not adequately protect their

Personal Information, they would not have provided, or allowed to have provided, their Personal Information to Defendant, nor would they have sought services or employment from Defendant.

354. Plaintiffs and Class members (or third-party agents) performed their obligations under the implied contract when they provided, directly or indirectly, Defendant with their Personal Information.

355. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class members' Personal Information and failing to provide them with timely and accurate notice of the Data Breach.

356. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Class members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and Class members' Personal Information.

COUNT FOUR
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Nationwide Class)

357. Plaintiffs reallege all previous paragraphs as if fully set forth herein.

358. In light of the special relationship between Defendant and Plaintiffs and Class members, whereby Defendant became guardian of Plaintiffs' and Class members' Personal Information, Defendant became a fiduciary by its undertaking and guardianship of the Personal Information, to act primarily for Plaintiffs and Class members (1) for the safeguarding of Plaintiffs' and Class members' Personal Information, (2) to timely notify Plaintiffs and Class members of the Data Breach, and (3) to maintain complete and accurate records of what information Defendant stores and where.

359. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them, in particular, to keep secure their Personal Information.

360. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give timely notice of the Data Breach.

361. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class members' Personal Information.

362. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injuries as alleged herein.

COUNT FIVE
VIOLATION OF THE MINNESOTA UNIFORM
DECEPTIVE TRADE PRACTICE ACT
Minn. Stat. § 325D.43-48
(On Behalf of Plaintiffs and the Nationwide Class)

363. Plaintiffs reallege all previous paragraphs as if fully set forth herein.

364. The Minnesota Uniform Deceptive Trade Practice Act, Minn. Stat. § 325D.43-48 ("MDUPTA") prohibits deceptive trade practices in person's business, vocation, or occupation. *See* Minn. Stat. § 325D.44(1).

365. MDUPTA applies to Defendant because Defendant advertised, offered, sold, and/or provided goods or services in Minnesota.

366. Defendant violated MDUPTA by, *inter alia*:

- a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Personal Information, which was a direct and proximate cause of the Data Breach;

- b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681e, and the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Data Breach;
- d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Personal Information; and
- e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

367. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their Personal Information.

368. Defendant intended to mislead Plaintiffs and Class members and induce them to rely on its omissions.

369. Had Defendant disclosed to Plaintiffs and Class members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the Personal Information that Plaintiffs and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

370. Defendant intentionally, knowingly, maliciously, and recklessly disregarded Plaintiffs' and Class members' rights.

371. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

372. Additionally, on information and belief, Plaintiffs' Personal Information has already been published on the dark web by cybercriminals, including at least the ShinyHunters ransomware gang.

373. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law.

COUNT SIX
VIOLATION OF THE MINNESOTA HEALTH RECORDS ACT
Minn. Stat. § 144.291, et seq.
(On Behalf of Plaintiffs and the Nationwide Class)

374. Plaintiffs reallege all previous paragraphs as if fully set forth herein.

375. Under the Minnesota Health Records Act (MHRA), “health record” means any information, whether oral or recorded in any form or medium that relates to the past, present, or future physical or mental health or condition of a patient; the provision of healthcare to a patient; or the past, present, or future payment of provision of healthcare to a patient. Minn. Stat. § 144.291, subd. 2(c).

376. The Personal Information of Plaintiffs and Class members that was compromised in the Data Breach falls within the MHRA’s definition of “health records”

377. Plaintiffs Rath, Jennings, Loughry, Buckner, Riley, Holmes, Kennedy, Lindley, and Spano, as well as Class members are “patients” as that term is defined in the MHRA at all times relevant under Minn. Stat. §144.291, subd. 2(g).

378. Under the MHRA, it is unlawful for a third party to access a patient’s health records from a provider, or a person who receives records from a provider, without the patient or the patient’s legally authorized representative’s consent, specific authorization in law, or a representative from a provider that holds written consent from the patient authorizing the release. Minn. Stat. § 144.293, subd. 2(1-3).

379. Through the Data Breach, Defendant released Plaintiffs’ and Class members’ Personal Information, including their health records, to cybercriminals.

380. Neither Plaintiffs nor Class members consented to have their records released to cybercriminals.

381. Defendant’s release of Plaintiffs’ and Class members’ Personal Information constitutes an “affirmative” release under Minnesota law. *See Larson v. Nw. Mut. Ins. Co.*, 855 N.W.2d 293, 302 (Minn. 2014).

382. Under the MHRA, a provider or other person who causes an unauthorized release of a health record by negligently or intentionally releasing the health record is liable to the patient

for compensatory damages, plus costs and reasonable attorneys' fees. Minn. Stat. § 144.298, subd. 2.

383. Defendant's release of Plaintiffs' and Class members' health information directly and proximately caused them actual, tangible, injury-in-fact and damages as alleged herein.

384. Pursuant to the MHRA, Plaintiffs and Class members are entitled to recover compensatory damages plus costs and reasonable attorneys' fees.

COUNT SEVEN
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY
OF MEDICAL INFORMATION ACT
Cal. Civ. Code § 56, *et seq.*
(On Behalf of Plaintiffs Loughry, Egbert, and the California Subclass)

385. Plaintiffs Loughry and Egbert reallege all previous paragraphs as if fully set forth herein and bring this claim on behalf of themselves and the California Subclass (the "Class" for the purposes of this count).

386. Defendant is "a provider of health care," as defined in Cal. Civ. Code §56.05(m) and is therefore subject to the requirements of the California Confidentiality of Medical Information Act (CMIA), Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

387. At all relevant times, Defendant was a provider of health care because it had the "purpose of maintaining medical information to make the information available to the individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manager his or her information, or for the diagnosis or treatment of the individual."

388. As a provider of health care or a contractor, Defendant is required by the CMIA to ensure that medical information regarding patients is not disclosed, disseminated, and/or released without patients' authorization, and to protect and preserve the confidentiality of patients' medical

information under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

389. As a provider of health care or a contractor, Defendant is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

390. Defendant is a person/entity licensed under California's Business and Professions Code, Division 2. *See* Cal. Bus. Prof. Code § 4000, *et seq.*

391. Plaintiffs Loughry, Egbert, and the Class are "patients" as defined in CMIA, Cal. Civ. Code § 56.05(k) ("Patient" means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains."). Furthermore, Plaintiffs Loughry, Egbert, and the Class, as patients of Defendant, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network, and were patients on or before the date of the Data Breach.

392. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Defendant, which allowed the hackers to see and obtain the Personal Information of Plaintiffs Loughry, Egbert, and the Class.

393. Defendant negligently created, maintained, preserved, stored, and then exposed Plaintiffs Loughry's, Egbert's, and the Class's individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiffs Loughry's, Egbert's, and the Class's names, contact information, dates of birth, Social Security numbers, and health-related information, which alone or in combination with other publicly available information reveals their

identities. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that allowed unauthorized parties to access, exfiltrate, and actually view the Personal Information of Plaintiffs Loughry, Egbert, and the Class.

394. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiffs Loughry, Egbert, and the Class to unauthorized persons and the breach of the confidentiality of that information. Defendant negligently failed to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs Loughry's, Egbert's, and the Class's medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

395. Plaintiffs Loughry's, Egbert's, and the Class's medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

396. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of Defendant's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiffs Loughry, Egbert, and the Class have suffered (and will continue to suffer) injuries as alleged herein.

397. Plaintiffs Loughry, Egbert, and the Class were injured and have suffered damages, as described above, from Defendant's illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of \$1,000, punitive damages of \$3,000, injunctive relief, and attorneys' fees, expenses and costs.

COUNT EIGHT
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a)
(On Behalf of Plaintiffs Loughry, Egbert, and the California Subclass)

398. Plaintiffs Loughry and Egbert reallege all previous paragraphs as if fully set forth herein and bring this claim on behalf of themselves and the California Subclass (the “Class” for the purposes of this count).

399. The California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

400. Defendant is a “business” under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of \$25 million.

401. Plaintiffs Loughry, Egbert, and the Class are covered “consumers” under § 1798.140(g) in that they are natural persons who are California residents.

402. Upon information and belief, the Personal Information of Plaintiffs Loughry, Egbert, and the Class at issue in this lawsuit constitutes “personal information” under § 1798.150(a) and 1798.81.5, in that the Personal Information Defendant collects and which was

impacted by the Data Breach includes individuals' first names or first initial and last names in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security numbers and (ii) health information.

403. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs Loughry's, Egbert's, and the Class's Personal Information and that the risk of a data breach was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to protect the Personal Information of Plaintiffs Loughry, Egbert, and the Class. Specifically, Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information it store subjected Plaintiffs Loughry's, Egbert's, and the Class's nonencrypted and nonredacted Personal Information to unauthorized access and exfiltration, theft, or disclosure.

404. As a direct and proximate result of Defendant's acts, Plaintiffs Loughry, Egbert, and the Class were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their Personal Information, stress, fear, and anxiety, nominal damages, and additional losses as described herein.

405. Section 1798.150(b) specifically provides that "[n]o [pre]filing notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

406. Pursuant to California Civil Code § 1798.150(b), Plaintiffs Loughry and Egbert mailed CCPA notice letters to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiffs Loughry and Egbert believe such cure is not possible under these facts and circumstances—then they intend to promptly amend this Consolidated Class Action Complaint to seek statutory damages as permitted by the CCPA.

407. Accordingly, Plaintiffs Loughry, Egbert, and the Class seek actual pecuniary damages suffered as a result of Defendant's violations described herein.

COUNT NINE
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW (UCL)
CAL BUS. & PROF. CODE § 17200, *et seq.*
(On Behalf of Plaintiffs Loughry, Egbert, and the California Subclass)

408. Plaintiffs Loughry and Egbert reallege all previous paragraphs as if fully set forth herein and bring this claim on behalf of themselves and the California Subclass (the "Class" for the purposes of this count).

409. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq.* (UCL), which prohibits unlawful, unfair, or fraudulent business acts or practices.

410. Defendant's conduct is unlawful because it violates the CMIA, CCPA, Civ. Code § 1798.100, *et seq.*, HIPAA, and Section 5(a) of the FTCA.

411. Defendant stored the Personal Information of Plaintiffs Loughry, Egbert, and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept such Personal Information secure.

412. Defendant failed to disclose to Plaintiffs Loughry, Egbert, and the Class that their Personal Information was not secure. However, Plaintiffs Loughry, Egbert, and the Class were entitled to assume, and did assume, that Defendant had secured their Personal Information. At no time were Plaintiffs Loughry, Egbert, and the Class on notice that their Personal Information was not secure, which Defendant had a duty to disclose.

413. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access

and exfiltration, theft, or disclosure of Plaintiffs Loughry's, Egbert's, and the Class's nonencrypted and nonredacted Personal Information.

414. Had Defendant complied with these requirements, Plaintiffs Loughry, Egbert, and the Class would not have suffered the damages related to the Data Breach.

415. Defendant's conduct was unlawful, in that it violated the CCPA.

416. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the FTCA.

417. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

418. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting Personal Information.

419. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

420. Defendant made the Personal Information of Plaintiffs Loughry, Egbert, and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting them to an impending risk of identity theft.

421. As a result of those unlawful and unfair business practices, Plaintiffs Loughry, Egbert, and the Class suffered injury-in-fact and have lost money or property.

422. The injuries to Plaintiffs Loughry, Egbert, and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

423. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged herein.

424. Therefore, Plaintiffs Loughry, Egbert, and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT TEN
DECLARATORY RELIEF
(On Behalf of Plaintiffs and the Nationwide Class)

425. Plaintiffs reallege all previous paragraphs as if fully set forth below.

426. The Declaratory Judgments Act, 28 U.S.C. §§ 2201, *et seq.* authorizes courts to declare rights, status, and other legal relations so as to afford litigants relief from uncertainty and insecurity.

427. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective duties to reasonably safeguard Plaintiffs' and Class members' Personal Information, and whether Defendant is currently maintaining data security

measures adequate to protect Plaintiffs and Class members from future data breaches that compromise their Personal Information.

428. The Data Breach evidences Defendant's failure to provide security measures that were adequate, reasonable, and/or compliant with industry standards and best practices with regard to safeguarding Plaintiffs' and Class members' Personal Information.

429. The Data Breach and Defendant's response to it demonstrate that its systems remain vulnerable to unauthorized access, and more stringent measures must be taken to safeguard the Personal Information of Plaintiffs and Class members going forward.

430. Indeed, as a result of the Data Breach, the ransomware gang ShinyHunters now possess detailed knowledge as to how to successfully infiltrate Defendant's systems, and thus may commit additional data breaches against Defendant. Any additional Personal Information Defendant collects and retains regarding its patients and employees, including Plaintiffs' and Class members', is now vulnerable to future breaches by ShinyHunters or other bad actors to whom ShinyHunters discloses its methods.

431. Plaintiffs seek a declaration that Defendant's current security measures are inadequate to safeguard Personal Information, do not comply with its obligations to keep Personal Information secure, and that Defendant must implement specific additional security practices to provide reasonable protection and security for the Personal Information it maintains, including the Personal Information of Plaintiffs and Class members.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

- a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class

requested herein;

- b. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:
 - i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
 - ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
 - iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
 - iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;
 - v. Ordering that Defendant cease transmitting Personal Information via unencrypted email;
 - vi. Ordering that Defendant cease storing Personal Information in email accounts;
 - vii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provision of

services;

- viii. Ordering that Defendant conduct regular database scanning and securing checks;
 - ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
 - x. Ordering Defendant to meaningfully educate its current, former, and future employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences.
- c. An order requiring Defendant to pay the costs involved in notifying Class members about the judgment and administering the claims process.
 - d. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, restitution, pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and
 - e. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

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

Dated: July 24, 2026

/s/Daniel E. Gustafson
Daniel E. Gustafson (#202241)
David A. Goodwin (#386715)

Joe E. Nelson (#402378)
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 So. Sixth Street, Suite 2600
Minneapolis, MN 55402
Telephone: (612) 333-8844
Fax: (612) 339-6622
dgoodwin@gustafsongluek.com
dgustafson@gustafsongluek.com
jnelson@gustafsongluek.com

Raina C. Borrelli (SBN 032127)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

Kate M. Baxter-Kauf (MN Bar #0392037)
Karen Hanson Riebel (MN Bar #219770)
Jacob E. Lanthier (MN ID #401845)
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
jelanthier@locklaw.com

Melissa S. Weiner (MN Bar 0387900)
Ryan T. Gott (MN Bar No. 0397978)
PEARSON WARSHAW, LLP
328 Barry Avenue S., Suite 200
Wayzata, Minnesota 55391
Telephone: (612) 389-0600
Fax: (612) 389-0610
mweiner@pwfirm.com
rgott@pwfirm.com

Brian C. Gudmundson (MN Bar #0336695)
Michael L. Laird (MN Bar No. 0398436)
Madison M. DeMaris (MN Bar No. 0403467)
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400

brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
madison.demaris@zimmreed.com

Nicole S. Frank (#0388822)
**BRADFORD ANDRESEN NORRIE &
CAMAROTTO**
3600 American Blvd. West, Ste. 670
Bloomington, MN 55431
Tel: (612) 474-1811
nfrank@banclaw.com

Rebecca A. Peterson (MN Bar #392663)
Krista K. Freier (MN Bar #390223)
Catherine A. Peterson (MN Bar #505172)
HECHT PARTNERS LLP
1650 West 82nd Avenue
Suite 880
Bloomington, MN 55431
Phone: (612) 778-9595
Facsimile: (888) 421-4173
rpeterson@hechtpartners.com
kfreier@hechtpartners.com
cpeterson@hechtpartners.com

Garrett D. Blanchfield (MN Bar #209855)
Brant D. Penney (MN Bar #316878)
**REINHARDT WENDORF &
BLANCHFIELD**
80 South 8th Street, Suite 900
Minneapolis, MN 55402
Tel: (651) 287-2100
g.blanchfield@rwblawfirm.com
b.penney@rwblawfirm.com

E Michelle Drake (MN Bar #0387366)
BERGER MONTAGUE PC
1229 Tyler Street NE
Suite 205
Minneapolis, MN 55413
Telephone: 612-594-5933
Facsimile: 612-584-4470
emdrake@bergermontague.com

*Proposed Interim Class Counsel and Counsel for
Plaintiffs and the Class*