UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION

CASE NO.: 1:25-cv-20117-RAR

ASHLEY OWINGS, ALEKSANDR MITERIN, AILEMA GASCON, BARBARA MASTEN, COURTNEY HOPPER, ROBERT OWEN, JEANNE AUER, JENNIFER CALDWELL-JOCK, and H.P. through her guardian Lauren G. Savener, on behalf of themselves, and all others similarly situated,

Plaintiffs,

v.

MEDUSIND, INC.,

Defendant.

JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Ashley Owings, Aleksandr Miterin, Ailema Gascon, Barbara Masten, Courtney Hopper, Robert Owen, Jeanne Auer, Jennifer Caldwell-Jock, and H.P. through her guardian Lauren G. Savener ("Plaintiffs") file this Consolidated Amended Class Action Complaint on behalf of themselves, and all others similarly situated, against Defendant Medusind, Inc. ("Defendant" or "Medusind"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE ACTION

1. This class action arises out of Defendant's failures to properly secure, safeguard, and adequately destroy Plaintiffs' and more than 360,000 other Class Members' sensitive personal identifiable information that it had acquired and stored for its business purposes.[1]

2. Defendant's data security failures allowed a targeted cyberattack to compromise Defendant's network ("Data Breach") that, upon information and belief, contained personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") of Plaintiffs and other individuals ("Class Members"). The Data Breach occurred on or around December 29, 2023. Defendant became aware of the Data Breach that day, but did not disclose it to Plaintiffs and Class Members until more than one year later, on January 7, 2025, when Plaintiffs and Class Members were sent letters in the mail from Defendant ("Notice Letter").[2]

3. Defendant is a medical and dental billing and software service provider. Defendant works with providers throughout the United States.[3]

4. Upon information and belief, Plaintiffs' and Class Members' Private Information was unlawfully accessed and may have been exfiltrated by a third party.

5. The Private Information compromised in the Data Breach included certain Private Information of patients whose Private Information was maintained by Defendant, including Plaintiffs.

6. On information and belief, a wide variety of Private Information was implicated in the breach, including for some individuals: names, home addresses, phone numbers, dates of birth,

[1] According to the Office of the Maine Attorney General, there are 360,934 victims of the Data Breach. *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/bf4aed39-d2f2-4ce2-bd56-5357107d7f3c.html (last visited Feb. 6, 2025).
[2] Sample Notice Letter, available at https://www.documentcloud.org/documents/25481987-medusind-data-breach-notice/ (last visited Feb. 6, 2025).
[3] *See* https://www.medusind.com/ (last visited Feb. 6, 2025).

health insurance account information, Social Security numbers, provider taxpayer identification numbers, and clinical information.[4]

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for either treatment or employment, or both.

8. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure Private Information from those risks left that property in a dangerous condition.

9. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

10. Defendant through its privacy policy, both expressly and impliedly understood its obligations and promised to safeguard Plaintiffs' and Class Members' Private Information.

[4] *See* Sample Notice Letter.

Plaintiffs and Class Members relied on these express and implied promises when seeking out and paying for Defendant's clients' services. But for this mutual understanding, Plaintiffs and Class Members would not have provided Defendant's clients with their Private Information. Defendant, however, did not meet these reasonable expectations, causing Plaintiffs and Class Members to suffer injury.[5]

11. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and full notice of the Data Breach.

12. In addition, Defendant failed to properly monitor the computer network and systems that housed the Private Information. Had it properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals a period of unimpeded access to the Private Information of Plaintiffs and Class Members.

13. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

14. As a result of the Data Breach, Plaintiffs and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiffs and Class Members must now and for years into the future closely monitor their medical and financial accounts to guard against

[5] https://www.medusind.com/about-medusind/ (last visited Feb. 6, 2025).

identity theft. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiffs and Class Members have suffered numerous actual and concrete injuries and damages.

15. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiffs' and Class Members' Private Information was targeted, accessed, viewed, has been misused, and disseminated on the Dark Web.

16. Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

17. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (g) deprivation of value of their Private Information; and (h) the continued risk to their sensitive Private 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 collected and maintained.

18. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

19. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence and negligence *per se*; (ii) breach of third-party beneficiary contract; (iii) unjust enrichment; (iv) violation of the California Confidentiality of Medical Information Act; (v) violation of the California Consumer Privacy Act; (vi) violation of the California Customer Records Act; and (vii) declaratory and injunctive relief.

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

PARTIES

21. Plaintiff Ashley Owings is an adult individual who at all relevant times has been a citizen and resident of California.

22. Plaintiff Aleksandr Miterin is an adult individual who at all relevant times has been a citizen and resident of Florida.

23. Plaintiff Ailema Gascon is an adult individual who at all relevant times has been a citizen and resident of Florida.

24. Plaintiff Barbara Masten is an adult individual who at all relevant times has been a citizen and resident of Florida.

25. Plaintiff Courtney Hopper is an adult individual who at all relevant times has been a citizen and resident of North Carolina.

26. Plaintiff Robert Owen is an adult individual who at all relevant times has been a citizen and resident of Arkansas.

27. Plaintiff Jeanne Auer is an adult individual who at all relevant times has been a citizen and resident of California.

28. Plaintiff Jennifer Caldwell-Jock is an adult individual who at all relevant times has been a citizen and resident of Wisconsin.

29. Plaintiff H.P., through her guardian Lauren G. Savener, is a minor individual who at all relevant times has been a citizen of Kansas.

30. Defendant Medusind Inc. is a Florida corporation with its headquarters and principal place of business located at 6100 Blue Lagoon Drive, Suite 450, Miami, Florida 33126. Upon information and belief, Defendant's clients' patients and the victims of the Data Breach reside in multiple states, including Florida.

JURISDICTION AND VENUE

31. This Court has subject-matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, some of whom have different citizenships from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

32. This Court has personal jurisdiction over Defendant because it is a Florida corporation with its headquarters and principal place of business in Florida.

33. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District, maintains Plaintiffs' and Class Members' Private Information in this District, and has caused harm to Plaintiffs and Class Members in this District.

FACTUAL ALLEGATIONS

A. Defendant's Business

34. Defendant provides customized medical billing software for a variety of health care providers, including dentists, who contracted with Defendant and provided it with their patients'—Plaintiffs' and Class Members'—Private Information. On information and belief, more than 6,000 healthcare providers throughout the United States use Defendant's billing software.[6]

35. In addition to a medical billing platform, Defendant's software products aim to give providers insight into revenue and help optimize costs.[7]

36. Defendant advertises on its website as follows:

> Medusind is much more than a billing service. Medusind becomes our client's Revenue Cycle partner in every sense of the word. Team Leaders and Department Heads provide unwavering leadership to their passionate and capable RCM service delivery teams whose sole purpose is to improve the financial performance and adhere to all compliance regulations and guidelines to mitigate exposure for our customers.[8]

37. As part of its business, Defendant collects and stores Plaintiffs' and Class Members' Private Information on its computer systems (which on information and belief are located in Florida), including, *inter alia*, patients' full names, home address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

38. When Defendant collects this Private Information, it promises to use reasonable care to protect and safeguard the Private Information, from unauthorized disclosure.

---

[6] https://www.bitdefender.com/en-us/blog/hotforsecurity/attack-against-medical-billing-company-medusind-exposes-data-of-360-000-people (last visited Feb. 6, 2025).
[7] *E.g.*, https://www.medusind.com/medclarity-practice-management-software/ (last visited Feb. 6, 2025).
[8] https://www.medusind.com/about-medusind/ (last visited Feb. 6, 2025).

B. The Data Breach

39. According to Defendant's Notice Letter, on or around December 29, 2023, Defendant experienced a cyberattack to its computer information technology systems by an "unauthorized threat actor," which resulted in the unauthorized disclosure and exfiltration of patients' Private Information, including of Plaintiffs and Class Members, including health insurance and billing information (such as insurance policy numbers or claims/benefits information), payment information (such as debit/credit card numbers or bank account information), health information (such as medical history, medical record number, or prescription information), government identification (such as Social Security number, taxpayer ID, driver's license, or passport number), and other personal information (such as date of birth, email, address, or phone number).[9]

40. The Notice of Data Breach states sent to Plaintiffs and Class Members states:

> You are receiving this letter because your information may have been impacted by a cyber incident experienced by Medusind, Inc. ("Medusind") that took place on December 29, 2023, and that we discovered later the same day. Medusind is a revenue cycle management company that provides billing support to health care organizations, including your health care provider. Through an investigation, Medusind determined that information belonging to you may have been accessed without authorization. The purpose of this letter is to give you an overview of the data security incident, our response to it, and let you know about the support we are offering to you.
>
> **What Happened?**
> On December 29, 2023, Medusind discovered suspicious activity within its IT network. Upon discovering the suspicious activity, Medusind took the affected systems offline and hired a leading cybersecurity forensic firm to conduct an investigation. Through this investigation, we found evidence that a cybercriminal may have obtained a copy of certain files containing your personal information. Additionally, we implemented enhanced security

[9] Sample Notice Letter.

measures to prevent similar incidents from occurring in the future.
[10]

41. In addition, in its Notice of Data Breach, Defendant offered complimentary credit monitoring through Kroll for two years.[11] Defendant's offer of credit monitoring as part of the Data Breach notice further highlights the inherent risk of identity theft Plaintiffs and Class Members face due to the Data Breach.

42. The Notice of Data Breach did not further elaborate on the nature or extent of the Data Breach, omitting its scope or size.

43. Defendant waited more than ***one year*** to inform affected current and former patients of the unauthorized disclosure of their Personal Dara Breach in the Data Breach, waiting until January 7, 2025, to provide written notice to Plaintiffs and Class Members.

44. Defendant's conduct, by acts of commission or omission, caused the Data Breach, including: Defendant's failures to implement best practices and comply with industry standards concerning computer system security to adequately safeguard patient Private Information, allowing Private Information to be accessed and stolen, and by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach, and by failing to adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems, resulting in the Data Breach.

45. On information and belief, as more fully articulated below, Plaintiffs and Class Members' Private Information, was unauthorizedly disclosed to, and actually exfiltrated by, third-party cybercriminals in the Data Breach, has now or will imminently be posted to the Dark Web

[10] *Id.*
[11] *Id.*

for public viewing and use, in the public domain, and/or utilized for criminal and fraudulent purposes and misuse.

C. Defendant Knew the Risks of Storing Valuable Private Information, Including Patient PHI, and the Foreseeable Harm to Victims.

46. At all relevant times, Defendant knew it was storing and permitting its employees to use its internal network server to transmit valuable, sensitive Private Information, including patient PHI, and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

47. Defendant also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

48. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

49. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[12] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

50. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the ITRC, in 2019, there were 1,473 reported

[12] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited Feb. 6, 2025).

data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[13]

51. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[14]

52. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[15]

53. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily—making the industry a growing target."[16]

54. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's clients' patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

55. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even

---

[13] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.

[14] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).

[15] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.

[16] *Id.*

seen $60 or $70."[17] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.18.

56. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[19]

57. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can **sell for up to $1,000 online.**"[20]

---

[17] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[18] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[19] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[20] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

58. 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 has been sold or posted on the [Dark] 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."21

59. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

D. Defendant Breached its Duty to Protect Its Patients' Private Information.

60. As an entity collecting, maintaining, and profiting off Plaintiffs' and Class Members' highly sensitive Private Information, Defendant had a duty to exercise reasonable care and comply with applicable industry standards and statutory security requirements to protect their information.

61. Indeed, Defendant was on notice that it was maintaining highly valuable data, which it knew was at risk of being targeted by cybercriminals, and knew of the extensive harm that would occur if Plaintiffs' and Class Members' Private Information was exposed through a data breach.

[21] United States Government Accountability Office, Report to Congressional Requesters, Private Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

62. Because Plaintiffs and Class Members provided their Private Information to their respective providers who in turn provided that information to Defendant, Defendant had a special relationship with Plaintiffs and Class Members which provided an independent duty of care. Defendant owed a duty to use reasonable security measures because it undertook to collect, store, and use customers' Private Information.

63. Upon information and belief, Defendant's HIPAA Privacy Policy is provided or made available to every one of its clients' patients both prior to receiving treatment, and upon request.[22]

64. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA"). Under state and federal law, businesses like Defendant have duties to protect its clients' current and former patients' Private Information and to notify them about breaches.

65. Specifically, Defendant declares:

> Medusind has designed and implemented an Information Security Management System that is based on ISO/IEC 27001: 2013 standard and is in compliance with the Health Insurance Portability and Accountability Act (HIPAA). Our ISO 27001: 2013 Certification adds strength and security to our total business practice by providing strict quality standards and a solid framework of management controls.
>
> Our internal compliance training and certifications programs provide a basis for best practices and enhances compliance awareness and adherence company-wide. Medusind's well-developed compliance culture is reinforced through continuous employee training and education on information security, PHI, and related compliance topics.[23]

[22] *See* https://www.medusind.com/about-medusind/ (last visited Feb. 6, 2025).
[23] *Id.*

66. The Private Information held by Defendant in its computer system and network included the highly sensitive Private Information of Plaintiffs and Class Members.

67. Despite holding Private Information for millions of individuals, Defendant failed to adopt reasonable data security measures to prevent and detect unauthorized access to their highly sensitive databases, putting their customers' highly sensitive information at risk.

68. Defendant failed to properly implement data security practices that were reasonable and up to industry standards.

E. Defendant Failed to Comply with Regulatory Requirements and Industry Practices.

69. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and the healthcare sector. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

70. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain Private Information, about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access. Florida is one such state and requires that entities like Defendant "take reasonable measures to protect and secure data in electronic form containing personal information." Fla. Stat. § 501.171(2).

71. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems setting up network systems such as firewalls, switches,

and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.[24]

72. The Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[25]

73. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.26 The guidelines note businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct 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.

74. The FTC also recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious

---

[24] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security [https://perma.cc/NY6X-FUY].

[25] *Start With Security*, FED. TRADE COMM'N, at 2, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Aug. 22, 2023).

[26] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N, https://www.ftc.ov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 22, 2023).

activity on the network; and verify that third-party service providers have implemented reasonable security measures.[27]

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

76. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC recognizes that failure to restrict access to information28 and failure to segregate access to information29 may violate the FTC Act.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data (*i.e.*, Private Information) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

78. Furthermore, Defendant is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

---

[27] *See Start With Security*, FED. TRADE COMM'N, *supra* n.48.
[28] *In the Matter of LabMD, Inc.*, Dkt. No. 9357, at 15 ("Procedures should be in place that restrict users' access to only that information for which they have a legitimate need."), https://www.ftc.gov/ system/files/documents/cases/160729labmd-opinion.pdf.
[29] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015) (stating that companies should use "readily available security measures to limit access between" data storage systems).

79. The Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.[30]

80. Pursuant to HIPAA's mandate that Defendant follow "applicable standards, implementation specifications, and requirements . . . with respect to electronic protected health information," 45 C.F.R. § 164.302. Defendant was required to, at minimum, 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), and "[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).

81. Defendant is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). See 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

82. Both HIPAA and HITECH obligate Defendant to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure

[30] *Summary of the HIPAA Security Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Aug. 22, 2023).

of sensitive patient Private Information. See 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. §17902.

83. As alleged in this Complaint, Defendant has failed to comply with HIPAA and HITECH. It has failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of protected health information.

84. Additionally, cybersecurity experts have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.[31] Defendant did not follow such minimum best practices.

COMMON INJURIES AND DAMAGES

85. As result of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

86. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, 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 but not limited to: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time

[31] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security/ [https://perma.cc/NY6X-TFUY].

and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

A. The Risk of Identity Theft to Plaintiffs and Class Members Is Present and Ongoing.

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

88. 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 the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

89. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information

through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

90. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[32] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.33 This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

91. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here.[34] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[35] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[36]

---

[32] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[33] *Id.*
[34] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[35] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[36] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

92. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[37]

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

94. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[38]

95. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name

---

[37] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

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

and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[39]

96. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[40]

97. One such example of criminals using PHI for profit is the development of "Fullz" packages. Cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

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

[39] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[40] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and Class Members' stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

99. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[41]

100. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[42] Defendant did not rapidly report to Plaintiffs and Class Members that their Private Information had been stolen.

101. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

102. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

103. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PHI. To protect themselves, Plaintiffs and Class

[41] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[42] *Id.*

Members will need to remain vigilant against unauthorized data use for years or even decades to come.

104. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[43]

105. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[44]

106. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to

[43] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

[44] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[45]

107. Defendant's failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

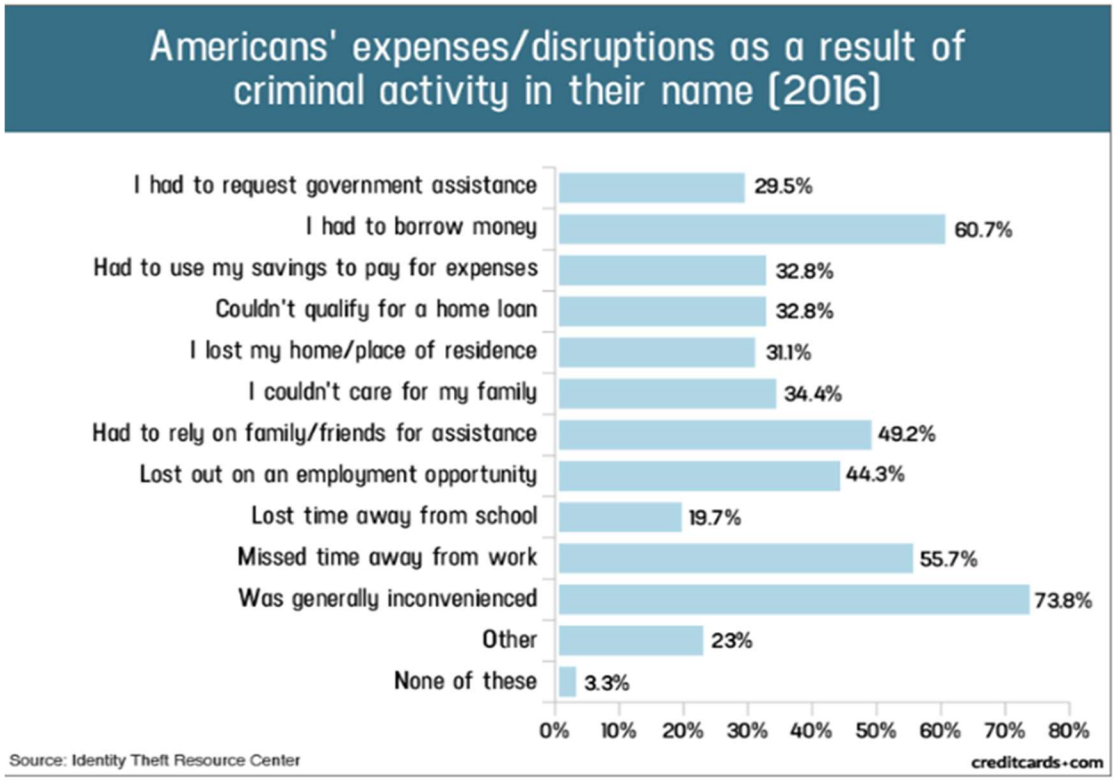
B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

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

109. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

[45] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices.

110. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[46]



111. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[47] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to

[46] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

[47] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[48]

C. Diminution of Value of the Private Information

112. Private Information is a valuable property right.[49] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

113. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

114. Private Information can sell for as much as $363 per record according to the Infosec Institute.[50]

115. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data was selling on the dark web for $50 and up.[51]

---

[48] *See* https://www.identitytheft.gov/Steps.

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

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

[51] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

116. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[52] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[53,54] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[55]

117. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

D. Future Cost of Credit and Identify Theft Monitoring Is Reasonable and Necessary.

118. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damage they have suffered as a result of the Data Breach. Defendant has not offered any other relief or protection.

119. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the modus operandi of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to

[52] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[53] https://datacoup.com/.
[54] https://digi.me/what-is-digime/.
[55] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

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

121. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[56] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

122. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

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

[56] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

E. Loss of Benefit of the Bargain

124. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to provide their Private Information, which was a condition precedent to obtain services, and paying Defendant for its services, Plaintiffs as consumers understood and expected that they were, in part, paying for services and data security to protect the Private Information required to be collected from them.

125. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

F. Injunctive Relief Is Necessary to Protect Against Future Data Breaches.

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

127. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, inter alia, monetary losses and lost time. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Private Information; and

h. continued risk to their Private Information —which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

G. Lack of Compensation

128. Defendant's credit monitoring offer fails to sufficiently compensate victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

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

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

131. Further, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills

opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

132. Specifically, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

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

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

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

g. Placing "freezes" and "alerts" with credit reporting agencies;

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

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

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

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

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

133. In addition, Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the property of loss of value damages in related cases.

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

135. Defendant's more than one year delay in reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of Private Information. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach and had not formally notified victims. They have yet to offer an explanation for the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiffs and Class Members.

PLAINTIFFS' EXPERIENCES

Ashley Owings' Experience

136. Plaintiff Ashley Owings (for the purposes of this section, "Plaintiff") is an adult individual who at all relevant times has been a citizen and resident of California.

137. Plaintiff is a patient of a health care provider that outsources information to Medusind and her information was stored with and handled by Defendant as a result of her dealings with her health care provider.

138. As a patient of her healthcare provider, she was required to provide her PII and PHI which was subsequently provided to Defendant, including among other things, her full name,

address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

139. On or about January 7, 2025, Plaintiff received a Notice Letter from Defendant, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including her health insurance and billing information (such as insurance policy numbers or claims/benefits information), payment information (such as debit/credit card numbers or bank account information), health information (such as medical history, medical record number, or prescription information), government identification (such as driver's license or passport number), and other person information (such as date of birth, email, address, or phone number).

140. Plaintiff diligently protects her Private Information.

141. Plaintiff is not aware of ever being part of a data breach involving her medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including increasingly reviewing her credit monitoring service, setting up notices and reports and carefully reviewing all her accounts.

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

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

144. Plaintiff has suffered actual injury in that an unauthorized third party attempted to open a credit card in her name.

145. Plaintiff has suffered actual injury in that an unauthorized third party attempted to withdraw money from her bank accounts.

146. Plaintiff has additionally suffered injury in that she has had to close bank accounts and receive credit cards with new account numbers as a result of attempted fraud which upon information and belief resulted from the Data Breach.

147. Plaintiff has also suffered an actual injury in that she received notification that her Private Information was on the dark web.

148. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information in the Data Breach.

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

150. Plaintiff greatly values her privacy, and would not have provided her Private Information, undertaken the services and paid the amounts that she did if she had known that her Private Information would be maintained using inadequate data security systems.

Aleksandr Miterin's Experience

151. Plaintiff Aleksandr Miterin (for the purposes of this section" Plaintiff") is an adult individual who at all relevant times has been a citizen and resident of Florida.

152. Plaintiff is a patient of a health care provider that outsources information to Medusind and his information was stored with and handled by Defendant as a result of his dealings with his health care provider.

153. As a patient of his healthcare provider, he was required to provide his Private Information which was subsequently provided to Defendant, including among other things, his full name, address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

154. On or about January 7, 2025, Plaintiff received a Notice Letter from Defendant, informing him that his Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including his health insurance and billing information (such as insurance policy numbers or claims/benefits information), payment information (such as debit/credit card numbers or bank account information), health information (such as medical history, medical record number, or prescription information), government identification (such as driver's license or passport number), and other person information (such as date of birth, email, address, or phone number).

155. Plaintiff diligently protects his Private Information.

156. Plaintiff is not aware of ever being part of a data breach involving his medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, he has taken multiple steps to avoid identity theft, including increasingly reviewing

his credit monitoring service, setting up notices and reports and carefully reviewing all his accounts.

157. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors his Private Information multiple times a week and has already spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities. To date Plaintiff has spent approximately thirty (30) hours mitigating the impact of the Data Breach.

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

159. Plaintiff has additionally suffered actual injury in that an unauthorized third party attempted to withdraw money out of his bank account. Plaintiff has also discovered a balance increase on his credit card that was caused by an unauthorized third party. Upon information and believe these occurrences were as a direct result of the Data Breach.

160. Plaintiff has additionally suffered actual injury in the form of a notification from Experian that his Private Information was on the dark web. Upon information and belief this is a direct result of the Data Breach.

161. Plaintiff has additionally suffered actual injury in the form of fraud notifications from Experian and Credit Karma. Upon information and belief this is a direct result of the Data Breach.

162. Plaintiff has experienced a substantial increase in spam telephone calls from private phone numbers which upon information and belief are a direct result of the Data Breach.

163. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information in the Data Breach.

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

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

Ailema Gascon's Experience

166. Plaintiff Ailema Gascon (for the purposes of this section" Plaintiff") is an adult individual who at all relevant times has been a citizen and resident of Florida.

167. Plaintiff is a patient of a health care provider that outsources information to Medusind and her information was stored with and handled by Defendant as a result of her dealings with her health care provider.

168. As a patient of her healthcare provider, she was required to provide her Private Information which was subsequently provided to Defendant, including among other things, her full name, address, date of birth, Social Security number, driver's license or state ID number,

financial account and payment card information, medical information, and health insurance information.

169. On or about January 7, 2025, Plaintiff received a Notice Letter from Defendant, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including her health insurance and billing information (such as insurance policy numbers or claims/benefits information), payment information (such as debit/credit card numbers or bank account information), health information (such as medical history, medical record number, or prescription information), government identification (such as driver's license or passport number), and other person information (such as date of birth, email, address, or phone number).

170. Plaintiff diligently protects her Private Information.

171. Plaintiff is not aware of ever being part of a data breach involving her medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including increasingly reviewing her credit monitoring service, setting up notices and reports and carefully reviewing all her accounts.

172. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors her Private Information multiple times a week and has already spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities. To date Plaintiff has spent approximately five (5) hours mitigating the impact of the Data Breach.

173. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud. Upon information and belief, as a result of the Data Breach, Plaintiff has experienced increased amounts of spam email, texts and phones calls.

174. Plaintiff has additionally suffered actual injury in that an unauthorized third party attempted to withdraw $500 out of her bank account on or about February 2024. Plaintiff has also discovered a delivery charge on her credit card that was caused by an unauthorized third party. Upon information and believe these occurrences were as a direct result of the Data Breach.

175. Plaintiff has additionally suffered actual injury in the form of receiving multiple medical bills for services she did not receive in 2024. Upon information and belief this is a direct result of the Data Breach.

176. Plaintiff has experienced a substantial increase in spam telephone calls and texts which upon information and belief are a direct result of the Data Breach.

177. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information in the Data Breach.

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

179. Plaintiff greatly values her privacy, and would not have provided her Private Information, undertaken the services and paid the amounts that she did if she had known that her Private Information would be maintained using inadequate data security systems.

Barbara Masten's Experience

180. Plaintiff Barbara Masten (for the purposes of this section" Plaintiff") is an adult individual who at all relevant times has been a citizen and resident of Florida.

181. Plaintiff is a patient of a health care provider that outsources information to Medusind and her information was stored with and handled by Defendant as a result of her dealings with her health care provider.

182. As a patient of her healthcare provider, she was required to provide her Private Information which was subsequently provided to Defendant, including among other things, her full name, address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

183. On or about January 7, 2025, Plaintiff received a Notice Letter from Defendant, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including her health insurance and billing information (such as insurance policy numbers or claims/benefits information), payment information (such as debit/credit card numbers or bank account information), health information (such as medical history, medical record number, or prescription information), government identification (such as driver's license or passport number), and other person information (such as date of birth, email, address, or phone number).

184. Plaintiff diligently protects her Private Information.

185. Plaintiff is not aware of ever being part of a data breach involving her medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including increasingly reviewing her credit monitoring service, setting up notices and reports and carefully reviewing all her accounts.

186. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors her Private Information multiple times a week and has already spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities. To date Plaintiff has spent between seventeen (17) and twenty (20) hours mitigating the impact of the Data Breach.

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

188. Plaintiff has additionally suffered actual injury in that there were multiple unauthorized charges on her Visa account. Plaintiff was required to change her Visa account after every instance of fraud resulting in her having to change her account over five times.

189. Plaintiff has additionally suffered actual injury resulting from October/November 2024 charges appearing on her credit card that were made by an unauthorized third party. As a result, Plaintiff was required to close three separate accounts at the request of her bank/credit card

provider in December 2024. Upon information and believe these occurrences were as a direct result of the Data Breach.

190. Plaintiff has also suffered an actual injury in that she received a call in early January from the fraud department of her credit card advising her that an unauthorized caller claimed to be her and requested a credit limit increase. Upon information and belief this is a direct result of the Data Breach.

191. Plaintiff has experienced a substantial increase in spam telephone calls and texts which upon information and belief are a direct result of the Data Breach.

192. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information in the Data Breach.

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

194. Plaintiff greatly values her privacy, and would not have provided her Private Information, undertaken the services and paid the amounts that she did if she had known that her Private Information would be maintained using inadequate data security systems.

Courtney Hopper's Experience

195. Plaintiff Courtney Hopper (for the purposes of this section" Plaintiff") is an adult individual who at all relevant times has been a citizen and resident of North Carolina.

196. Plaintiff is a patient of a health care provider that outsources information to Medusind and her information was stored with and handled by Defendant as a result of her dealings with her health care provider.

197. As a patient of her healthcare provider, she was required to provide her Private Information which was subsequently provided to Defendant, including among other things, her full name, address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

198. On or about January 7, 2025, Plaintiff received a Notice Letter from Defendant, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including her health insurance and billing information (such as insurance policy numbers or claims/benefits information), payment information (such as debit/credit card numbers or bank account information), health information (such as medical history, medical record number, or prescription information), government identification (such as driver's license or passport number), and other person information (such as date of birth, email, address, or phone number).

199. Plaintiff diligently protects her Private Information.

200. Plaintiff is not aware of ever being part of a data breach involving her medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including increasingly reviewing her credit monitoring service, setting up notices and reports and carefully reviewing all her accounts.

201. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors her Private Information multiple times a week and has already

spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

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

203. Plaintiff has additionally suffered actual injury in that there were multiple unauthorized charges to her bank account which ultimately required her to close the account. As a result, she expended time information on various changing bill pay sites and working with the bank to dispute the charges. Plaintiff was never reimbursed for the fraudulent charges and also incurred overdraft fees of about $100 dollars because of the fraud.

204. Plaintiff has additionally suffered actual injury in that she received a $71.00 bill for medical services which she never obtained. To date she is still disputing the charges.

205. Plaintiff has also suffered an actual injury in that she received notification that her Private Information was on the dark web.

206. Plaintiff has experienced a substantial increase in spam telephone calls and texts which upon information and belief are a direct result of the Data Breach.

207. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information in the Data Breach.

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

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

209. Plaintiff greatly values her privacy, and would not have provided her Private Information, undertaken the services and paid the amounts that she did if she had known that her Private Information would be maintained using inadequate data security systems.

Robert Owens' Experience

210. Plaintiff Robert Owens (for the purposes of this section" Plaintiff") is an adult individual who at all relevant times has been a citizen and resident of Arkansas.

211. Plaintiff is a patient of a health care provider that outsources information to Medusind and his information was stored with and handled by Defendant as a result of his dealings with his health care provider.

212. As a patient of his healthcare provider, he was required to provide his Private Information which was subsequently provided to Defendant, including among other things, his full name, address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

213. On or about January 7, 2025, Plaintiff received a Notice Letter from Defendant, informing him that his Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including his health insurance and billing information (such as insurance policy numbers or claims/benefits information), payment information (such as debit/credit card numbers or bank account information), health information (such as medical history, medical record number, or prescription information), government identification (such as driver's license or passport number), and other person information (such as date of birth, email, address, or phone number).

214. Plaintiff diligently protects his Private Information.

215. Plaintiff is not aware of ever being part of a data breach involving his medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, he has taken multiple steps to avoid identity theft, including increasingly reviewing his credit monitoring service, setting up notices and reports and carefully reviewing all his accounts.

216. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors his Private Information multiple times a week and has already spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities. To date Plaintiff has spent approximately twenty to twenty-five (25) hours mitigating the impact of the Data Breach.

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

218. Plaintiff has additionally suffered actual injury in that an unauthorized third party used his bank information in Georgia. On or about May/June 2024 he received a fraud alert via text and was able to prevent the transaction from going through. There were four fraudulent charges attempted each for $11.00. Upon information and believe these occurrences were as a direct result of the Data Breach.

219. Plaintiff has additionally suffered actual injury in the form of a notification from CreditWise and his Capital One Quicksilver Card that his Private Information was on the dark web. Upon information and belief this is a direct result of the Data Breach.

220. Plaintiff has experienced a substantial increase in spam telephone calls from private phone numbers which upon information and belief are a direct result of the Data Breach. Some of the callers were requesting his social security number.

221. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information in the Data Breach. Additionally, Plaintiff has spent ten years building his credit from 480 to 740 and has fear and anxiety that ten years of work will be undone by cybercriminals as a result of the Data Breach.

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

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

Jeanne Auer's Experience

224. Plaintiff Jeanne Auer (for the purposes of this section" Plaintiff") is an adult individual who at all relevant times has been a citizen and resident of California.

225. Plaintiff is a patient of a health care provider that outsources information to Medusind and her information was stored with and handled by Defendant as a result of her dealings with her health care provider.

226. As a patient of her healthcare provider, she was required to provide her PII and PHI which was subsequently provided to Defendant, including among other things, her full name, address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

227. On or about January 7, 2025, Plaintiff received a Notice Letter from Defendant, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including her health insurance and billing information (such as insurance policy numbers or claims/benefits information), payment information (such as debit/credit card numbers or bank account information), health information (such as medical history, medical record number, or prescription information), government identification (such as driver's license or passport number), and other person information (such as date of birth, email, address, or phone number).

228. Plaintiff diligently protects her Private Information.

229. Plaintiff is not aware of ever being part of a data breach involving her medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including increasingly reviewing her credit monitoring service, setting up notices and reports and carefully reviewing all her accounts.

230. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors her Private Information multiple times a week and has already

spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

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

232. Plaintiff has suffered actual injury in that an unauthorized third party made two fraudulent withdrawals from her bank account on or about January 2025. Plaintiff keeps her debit card in a safe and secure location. Plaintiff was forced to spend time on the phone with her bank resolving the fraudulent transactions. Based upon information and belief, this was a result of the Data Breach.

233. Plaintiff has also suffered an actual injury in that she received notification that her Private Information was on the dark web.

234. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information in the Data Breach.

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

236. Plaintiff greatly values her privacy, and would not have provided her Private Information, undertaken the services and paid the amounts that she did if she had known that her Private Information would be maintained using inadequate data security systems.

Jennifer Caldwell-Jock's Experience

237. Plaintiff Jennifer Caldwell-Jock (for the purposes of this section" Plaintiff") is an adult individual who at all relevant times has been a citizen and resident of Wisconsin.

238. Plaintiff is a patient of a health care provider that outsources information to Medusind and her information was stored with and handled by Defendant as a result of her dealings with her health care provider.

239. As a patient of her healthcare provider, she was required to provide her Private Information which was subsequently provided to Defendant, including among other things, her full name, address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

240. On or about January 7, 2025, Plaintiff received a Notice Letter from Defendant, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including her health insurance and billing information (such as insurance policy numbers or claims/benefits information), payment information (such as debit/credit card numbers or bank account information), health information (such as medical history, medical record number, or prescription information), government identification (such as driver's license or passport number), and other person information (such as date of birth, email, address, or phone number).

241. Plaintiff diligently protects her Private Information.

242. Plaintiff is not aware of ever being part of a data breach involving her medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including increasingly reviewing

her credit monitoring service, setting up notices and reports and carefully reviewing all her accounts.

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

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

245. Plaintiff has additionally suffered actual injury in that there were multiple unauthorized attempts to open bank accounts in her name. Plaintiff placed a freeze on her credit as a result of the Data Breach, and therefore the attempts were unsuccessful.

246. Plaintiff has additionally suffered actual injury in that she has received notification of credit inquiries made by unauthorized third parties. Upon information and belief this was a direct result of the Data Breach.

247. Plaintiff has experienced a substantial increase in spam telephone calls and texts which upon information and belief are a direct result of the Data Breach.

248. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information in the Data Breach.

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

250. Plaintiff greatly values her privacy, and would not have provided her Private Information, undertaken the services and paid the amounts that she did if she had known that her Private Information would be maintained using inadequate data security systems.

H.P.' Experience

251. Plaintiff H.P. (for the purposes of this section, "Plaintiff") is a minor individual who at all relevant times has been a citizen and resident of Kansas. H.P. brings this action through her guardian Lauren G. Savener.

252. Plaintiff is a patient of a health care provider that outsources information to Medusind and her information was stored with and handled by Defendant as a result of her dealings with her health care provider.

253. As a patient of her healthcare provider, through her guardian, she was required to provide her PII and PHI which was subsequently provided to Defendant, including among other things, her full name, address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

254. On or about January 7, 2025, Plaintiff, through her guardian received a Notice Letter from Defendant, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach, including her health insurance and billing information (such as insurance policy numbers or claims/benefits information), payment

information (such as debit/credit card numbers or bank account information), health information (such as medical history, medical record number, or prescription information), government identification (such as driver's license or passport number), and other person information (such as date of birth, email, address, or phone number).

255. Plaintiff, through her guardian diligently protects her Private Information.

256. Plaintiff's guardian is not aware of Plaintiff ever being part of a data breach involving her medical records, health insurance or billing information and Plaintiff's guardian is concerned that it and other Private Information has now been exposed to bad actors. As a result, Plaintiff's guardian has taken multiple steps to avoid Plaintiff becoming a victim of identity theft, including increasingly reviewing credit monitoring services, setting up notices and reports and carefully reviewing accounts.

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

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

259. Furthermore, Plaintiff's guardian has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of her child's Private Information in the Data Breach.

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

261. Plaintiff's guardian greatly values her child's privacy, and would not have provided her child's Private Information, undertaken the services and paid the amounts that she did if she had known that her child's Private Information would be maintained using inadequate data security systems.

CLASS ALLEGATIONS

262. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as appropriate, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Class" or the "Nationwide Class"):

Nationwide Class

All individuals in the United States whose Private Information was compromised in the Defendant's Data Breach.

263. In addition, Plaintiffs Owings and Auer seek to represent a California subclass, defined as follows:

California Subclass

All individuals in California whose Private Information was compromised in the Defendant's Data Breach.

264. Excluded from the Classes are Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded

party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

265. Plaintiffs reserve the right to modify or amend the definition of the proposed Class and Subclasses prior to moving for class certification.

266. **Numerosity. Fed. R. Civ. P. 23(a)(1).** The Classes described above are so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. While the exact number of Class Members is unknown to Plaintiffs at this time, on information and belief, the Private Information of more than 360,000 individuals in the United States was compromised in the Data Breach.

267. **Predominance of Common Issues**. **Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2)'s commonality requirement and Rule 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

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

b. Whether Defendant's conduct violated the FTC Act and/or HIPAA;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including HIPAA and HITECH;

d. Whether Defendant's data security systems were consistent with industry standards;

e. Whether Defendant failed to take adequate and reasonable measures to ensure that its computer, applications, and data systems were protected and updated;

f. Whether Defendant failed to take available steps to prevent and stop the Data Breach from happening;

g. Whether Defendant owed tort duties to Plaintiffs and Class Members to protect their Private Information;

h. Whether Defendant owed a duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

i. Whether Defendant's delay in informing Plaintiffs and Class Members of the Data Breach was unreasonable;

j. Whether Defendant breached its duty to protect the Private Information of Plaintiffs and Class Members by failing to provide adequate data security;

k. Whether Defendant's failure to secure Plaintiffs' and Class Members' Private Information in the manner alleged violated federal, state and local laws, and/or industry standards;

l. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unauthorized access to and/or theft of Plaintiffs' and Class Members' Private Information;

m. Whether Defendant's conduct amounted to violations of state statutes, including the California Confidentiality of Medical Information Act, California Consumer Privacy Act, and California Customer Records Act;

n. Whether, as a result of Defendant's conduct, Plaintiffs and Class Members face a significant ongoing threat of identity theft, harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled;

o. Whether Defendant should retain the money paid by Plaintiffs and Class Members to protect their Private Information;

p. Whether Defendant should retain Plaintiffs' and Class Members' valuable Private Information; and

q. Whether, as a result of Defendant's conduct, Plaintiffs and Class Members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

268. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiffs' claims are typical of the claims of the Class Members. The claims of the Plaintiffs and members of the Classes are based on the same legal theories and arise from the same failure by Defendant to safeguard Private Information. Plaintiffs and Class Members were all patients of Defendant's clients, each having their Private Information obtained by an unauthorized third party.

269. **Adequacy of Representation. Fed. R. Civ. P. 23(a)(4).** Plaintiffs are adequate representatives of the Classes because their interests do not conflict with the interests of the other Class Members they seek to represent; Plaintiffs has retained counsel competent and experienced in complex class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

270. **Predominance. Fed. R. Civ. P. 23(b)(3).** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Classes. If Defendant breached its common law and statutory duties to secure Private Information on its network server, then Plaintiffs and each Class Member suffered damages from the exposure of sensitive Private Information in the Data Breach.

271. **Superiority. Fed. R. Civ. P. 23(b)(3).** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

272. **Manageability.** The precise size of the Classes is unknown without the disclosure of Defendant's records. The claims of Plaintiffs and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiffs and the Classes.

273. **Ascertainability**. All members of the proposed Classes are readily ascertainable. The Classes are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Classes. Defendant has access to information regarding which individuals were affected by the Data Breach and has already provided notifications to some of those people. Using this information, the members of the Classes can be identified, and their contact information ascertained for purposes of providing notice to the Classes.

274. **Particular Issues. Fed. R. Civ. P. 23(c)(4).** Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the

resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

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

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

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant breached a third-party beneficiary contract;

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

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

i. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and,

j. Whether Class Members are entitled to actual, consequential, statutory, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

275. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2) and (c).** Finally, class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole.

COUNT I
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class)

276. Plaintiffs restate and reallege paragraphs 1 through 275 above as if fully set forth herein.

277. Defendant owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

278. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

279. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

280. Defendant's duty also arose from Defendant's position as a medical billing and software provider. Defendant holds itself out as a trusted data collector and thereby assumes a duty to reasonably protect its clients' patients' information. Indeed, Defendant, as a direct data collector, was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

281. Defendant breached the duties owed to Plaintiffs and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices published to its customers.

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

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

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

285. Plaintiffs and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

286. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

287. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act was intended to guard against.

288. Defendant violated its own policies not to use or disclose PHI without written authorization.

289. Defendant violated its own policies by actively disclosing Plaintiffs' and the Class Members' PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI; failing to maintain the confidentiality of Plaintiffs' and the Class Members' records; and by failing to provide timely notice of the breach of PHI to Plaintiffs and the Class.

290. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their Private Information;

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

c. Costs associated with purchasing credit monitoring and identity theft protection services;

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

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Loss of their privacy and confidentiality in their PHI;

j. The erosion of the essential and confidential relationship between Defendant – as a medical billing and service provider – and Plaintiffs and Class Members as its clients' patients; and

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received.

291. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT II
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

292. Plaintiffs restate and incorporate by reference herein all the allegations contained in paragraphs 1 through 275.

293. Upon information and belief, Defendant entered into virtually identical contracts with its clients to provide billing and/or services, which included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

294. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

295. Defendant knew that if they were to breach these contracts with its clients, Plaintiffs and the Class would be harmed.

296. Defendant breached its contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

297. As foreseen, Plaintiffs and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

298. As a direct and proximate result of Defendant's breach of the third-party beneficiary contracts, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

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

299. Plaintiffs restate and incorporate by reference herein all the allegations contained in paragraphs 1 through 275.

300. This Count is pleaded in the alternative to Count II above.

301. Plaintiffs and Class Members conferred a benefit on Defendant by permitting their healthcare provider to turn over their Private Information to Defendant. Moreover, upon information and belief, Plaintiffs alleges that payments made by Defendant's clients to Defendant included payment for cybersecurity protection to protect Plaintiffs' and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiffs and Class Members in the form of elevated prices charged by Defendant's clients for their services. Plaintiffs and Class Members did not receive such protection.

302. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from payments made to it by its clients on behalf of Plaintiffs and Class Members.

303. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

304. Defendant has retained the benefits of its unlawful conduct, including the amounts of payment received indirectly from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

305. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it, which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

306. If Plaintiffs and Class Members had known that Defendant had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

307. Due to Defendant's conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendant to be permitted to retain the benefit of its wrongful conduct.

308. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control

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

309. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

COUNT IV
CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT
Cal. Civ. Code §§ 56 *et seq.* ("CMIA")
(On Behalf of Plaintiffs Owings and Auer and the California Subclass)

310. Plaintiffs Owings and Auer (for purposes of this count "Plaintiffs") restate and incorporate by reference herein all the allegations contained in paragraphs 1 through 275.

311. Defendant is a "contractor," as defined in Cal. Civ. Code § 56.05(d), and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.101(a) and (b).

312. Plaintiffs and California Subclass Members are "patients," as defined in CMIA, Cal. Civ. Code § 56.05(k).

313. Defendant disclosed "medical information," Plaintiffs are patients of a health care provider that outsources information to Medusind and their information was stored with and handled by Defendant as a result of her dealings with their health care provider.

314. As a patients of their healthcare provider, they were required to provide their PHI which was subsequently provided to Defendant.

315. Plaintiffs greatly value their privacy, and would not have provided their PHI, undertaken the services and paid the amounts that they did if they had known that their PHI would be maintained using inadequate data security systems. 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's employees, which allowed the hackers to see and obtain Plaintiffs' and California Subclass Members' medical information.

316. Defendant's negligence resulted in the release of PHI pertaining to Plaintiffs and California Subclass Members to unauthorized persons and the breach of the confidentiality of that information.

317. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and California Subclass Members' medical information in a manner that

preserved the confidentiality of the information contained therein is a violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

318. 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).

319. Plaintiffs and California Subclass Members were injured and have suffered damages, as described above, from Defendant's illegal 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, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

COUNT V
CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100 *et seq.* ("CCPA")
(On Behalf of Plaintiffs Owings and Auer and the California Subclass)

320. Plaintiffs Owings and Auer (for purposes of this count "Plaintiffs") restate and incorporate by reference herein all the allegations contained in paragraphs 1 through 275.

321. Defendant is a corporation organized or operated for the profit or financial benefit of its owners. Defendant collects consumers' Private Information (for the purposes of this section, "Private Information") as defined in the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.140.

322. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiffs' and California Subclass Members' nonencrypted Private Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

323. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiffs' and California Subclass Members' Private Information. As detailed herein, Defendant failed to do so.

324. As a direct and proximate result of Defendant's acts, Plaintiffs' and California Subclass Members' Private Information, including names, contact information, dates of birth, health insurance information, and other sensitive medical records, was subjected to unauthorized access and exfiltration, theft, or disclosure.

325. Plaintiffs and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter properly safeguards customer Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customer Private Information, including Plaintiffs' and California Subclass Members' Private Information. Plaintiffs and California Subclass Members have an interest in ensuring that their Private Information is reasonably protected.

326. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

327. Plaintiffs and California Subclass Members seek actual damages, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

328. On February 18, 2025, counsel for Plaintiffs provided written notice via certified mail to Defendant at its principal place of business of the intent to pursue claims under the CCPA and an opportunity for Defendant to cure. The domestic return receipt shows that Defendant received the letter. Plaintiffs' written notice set forth the violations of Defendant's duty to

implement and maintain reasonable security procedures and practices alleged in this Consolidated Class Action Complaint.

329. To date, Defendant has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiffs' counsel.

330. Plaintiffs and the California Subclass seek actual damages, as well as all monetary and non-monetary relief allowed by law, including statutory damages of up to $750 per customer per incident, actual financial losses; injunctive relief; and reasonable attorneys' fees and costs. *See* Cal. Civil Code § 1798.150.

COUNT VI
CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code §§ 1798.82 *et seq.* ("CCRA")
(On Behalf of Plaintiffs Owings and Auer and the California Subclass)

331. Plaintiffs Owings and Auer (for purposes of this count "Plaintiffs") restates and incorporates by reference herein all the allegations contained in paragraphs 1 through 275.

332. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay. . . ."

333. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately

following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

334. The CCRA specifies certain requirements when entities subject to its purview are required to issue a security breach notification, including that such entities do not unreasonably delay such notifications.

335. Defendant unreasonably delayed—by more than one year—before sending notice of the breach to California Subclass Members.

336. As a result of Defendant's violation of the CCRA, Plaintiffs and California Subclass Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiffs and California Subclass Members because their stolen information would have had less value to identity thieves.

337. As a result of Defendant's violation of the CCRA, Plaintiffs and California Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

COUNT VII
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

338. Plaintiffs restate and incorporate by reference herein all the allegations contained in paragraphs 1 through 275.

339. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 et seq., this Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to

restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

340. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs allege that Defendant's data security measures remain inadequate, contrary to Defendant's assertion that it has confirmed the security of its network. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of Private Information and remain at imminent risk that further compromises of Private Information will occur in the future.

341. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure its clients' patients' Private Information and to timely notify them of a data breach under the common law, HIPAA, and the FTC Act;

b. Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect patient Private Information; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure its clients' patients' Private Information.

342. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect patient Private Information in its possession, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

   i. engaging 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. engaging third-party security auditors and internal personnel to run automated security monitoring;

   iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

   iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

   v. conducting regular database scanning and security checks;

   vi. routinely and continually conducting 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

vii. meaningfully educating its clients and their patients about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

343. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

344. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

345. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus preventing future injury to Plaintiffs, Class Members, and others whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated, pray for relief as follows:

a. For an order certifying the Classes under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as the representatives of the Classes and Plaintiffs' attorneys as Class Counsel to represent the Classes;

b. For an order finding in favor of Plaintiffs and the Classes on all counts asserted herein;

c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

d. For an order of restitution, disgorgement, and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiffs' reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: February 18, 2025

Respectfully Submitted,

/s/ Mariya Weekes

Mariya Weekes (FL Bar # 56299)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2ND Floor
Coral Gables, FL 33134
Tele: 786-879-8200
mweekes@milberg.com

Jeff Ostrow (FL Bar No. 121452)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Ste. 500
Fort Lauderdale, Florida 33301
Tele: 954-525-4100
ostrow@kolawyers.com

Interim Class Counsel

Andrew J. Shamis
SHAMIS & GENTILE P.A.
14 NE 1st Avenue, Suite 705
Miami, Florida 33132
Tel: (305) 479-2299
ashamis@shamisgentile.com

Scott Edelsberg
Joseph Kanee
EDELSBERG LAW, P.A.
20900 NE 30th Ave.
Aventura, FL 33180
Tel: (305) 975-3320
scott@edelsberglaw.com
joseph@edelsberglaw.com

Marc H. Edelson*
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
T: (215) 867-2399
medelson@edelson-law.com

Manuel S. Hiraldo
HIRALDO P.A.
Florida Bar No. 030380
401 E. Las Olas Boulevard
Suite 1400
Ft. Lauderdale, Florida 33301
Email: mhiraldo@hiraldolaw.com
Telephone: 954.400.4713

Raina Borrelli*
STRAUSS BORRELLI, PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
raina@straussborrelli.com

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: dperry@masonllp.com
Email: lwhite@masonllp.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
T: (405) 389-4989
E: abm@murphylegalfirm.com

Jonathan S. Mann*
PITTMAN, DUTTON, HELLUMS, BRADLEY & MANN, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
E: jonm@pittmandutton.com

Counsel for Plaintiffs and the Putative Classes

**pro hac vice* application forthcoming

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing has been served via the CM/ECF system on all counsel of record on this 18th day of February, 2025.

/s/ Mariya Weekes
Mariya Weekes

ClassAction.org
