UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

ELENA GIRENKO, *individually and on behalf of all others similarly situated*, Plaintiff, v. THE MEDIBASE GROUP, INC., and STATEN ISLAND UNIVERSITY HOSPITAL, Defendants.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Elena Girenko ("Plaintiff") brings this Class Action Complaint on behalf of herself, and all others similarly situated, against Defendants, The Medibase Group, Inc. ("Medibase"), and Staten Island University Hospital ("Hospital") (collectively, "Defendants"), 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 Defendants' failures to implement reasonable and industry standard data security practices to properly secure, safeguard, and adequately destroy Plaintiff and Class Members' sensitive personal identifiable information that it had acquired and stored for its business purposes.

2. Medibase's data security failures allowed a targeted cyberattack to

compromise the networks of Staten Island University Hospital and other entities (the "Data Breach") that, upon information and belief, contained personally identifiable information ("PII")[1] and protected health information ("PHI")[2] (collectively, "Private Information") of Plaintiff and other individuals ("the Class"). The Data Breach occurred on or around January 26, 2024, Medibase notified Staten Island University Hospital on May 8, 2024, and began notifying the Class on July 5, 2024.[3]

3. Defendant Medibase provides healthcare solutions and services to healthcare providers across the country.[4]

4. Defendant Staten Island University Hospital provides health care services to patients in Staten Island, New York.[5]

5. According to the letter that Medibase sent to Plaintiff and Class

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103.

[3] https://www.jdsupra.com/legalnews/medibase-data-breach-leaks-staten-2060070/ (last visited June 11, 2024).

[4] https://medibase.com/about-us/ (last visited June 11, 2024).

[5] https://siuh.northwell.edu/ (las visited June 11, 2024).

Members (the "Notice Letter"), Medibase admits an unauthorized threat actor unlawfully accessed its systems.[6]

6. The Private Information compromised in the Data Breach included certain personal or protected health information of individuals whose Private Information was maintained by Defendants, including Plaintiff.

7. As disclosed in the Notice Letter, a wide variety of Private Information was implicated in the breach, including potentially: names, dates of birth, Social Security numbers, admit and discharge dates, outstanding balance amounts, and insurance information.[7]

8. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information which it was hired to protect.

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

---

[6] Plaintiff's Notice Letter, attached hereto as ***Exhibit A***; *see also* Exemplar Notice Letter, available at https://medibase.com/security-notice/ (last visited June 11, 2024).

[7] *Id*.

10. Upon information and belief, Defendants breached their 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 Plaintiff and Class Members of Defendants' 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.

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

Members with prompt and full notice of the Data Breach.

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

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

14. As a result of the Data Breach, Plaintiff and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their medical and financial accounts to guard against identity theft. As a result of Defendants' unreasonable and inadequate data security practices, Plaintiff 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 Plaintiff and Class Members' Private Information was targeted, accessed, has been misused, and disseminated on the Dark Web.

16. Plaintiff and Class Members must now closely monitor their financial

accounts to guard against future identity theft and fraud. Plaintiff 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. Plaintiff 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; (e) deprivation of value of their PII; and (f) the continued risk to their sensitive Private Information, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect it.

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

19. Accordingly, Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendants, and declaratory relief.

20. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiff and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

PARTIES

Plaintiff, Elena Girenko

21. Plaintiff Elena Girenko is, and at all times relevant hereto was, a citizen and resident of the state of New York.

22. Plaintiff was a patient of State Island University Hospital.

23. As a condition of receiving healthcare services from Hospital, she was required to provide her Private Information, directly or indirectly, to Defendants Medibase and Hospital, including among other things, her name, date of birth and Social Security number, and more.

24. At the time of the Data Breach–approximately January 2024, Defendants retained Plaintiff's Private Information in their systems.

25. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Plaintiff would not have entrusted her Private Information to Defendants had she known of Defendants' lax data security policies.

26. Plaintiff received the Notice Letter, by U.S. mail, from Defendant Medibase, dated July 5, 2024. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her Social Security number.

27. As a result of the Data Breach, and at the direction of Defendant Medibase's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, checking her credit monitoring services for fraud, signing up for the service offered and putting a freeze on his credit, changing passwords and logins, and considering whether to change her Social Security number. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

28. Plaintiff has also experienced an increased number of spam and suspicious calls, emails and texts following the Data Breach and believes that these may be phishing attempts designed to gain access to additional personal information.

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

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

31. 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.

32. As a result of the Data Breach, Plaintiff is at a present and continuing risk of identity theft for her lifetime. Plaintiff has a continuing interest in ensuring

that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Defendants

33. Defendant The Medibase Group, Inc. is a Georgia corporation with its principal place of business at 3205 S. Cherokee Lane, Suite 110 Woodstock, GA 30188. Upon information and belief, Medibase's customers and the victims of the Data Breach reside in multiple states, including New York.

34. Defendant Staten Island University Hospital is a New York corporation with its principal place of business at 475 Seaview Ave, Staten Island, NY 10305.

JURISDICTION AND VENUE

35. 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 citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

36. This Court has general personal jurisdiction over Medibase because it is a Georgia corporation that operates and has its principal place of business in this District.

37. This Court has specific personal jurisdiction over State Island University Hospital because it purposely availed itself of Georgia in using Medibase as a software solutions provider.

38. 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 Medibase is domiciled in this District and maintains Plaintiff's and Class Members' Private Information in this District.

FACTUAL BACKGROUND

A. Defendants Knew the Risks of Storing Valuable Private Information and the Foreseeable Harm to Victims.

39. At all relevant times, Defendants knew they were storing sensitive Private Information and that, as a result, Defendants' systems would be attractive targets for cybercriminals.

40. Defendants also knew that any breach of their 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.

41. 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.

42. 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."[8] 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.

43. 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 data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[9]

44. 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

[8] 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 June 11, 2024).

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

many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[10]

45. 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."[11]

46. "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."[12]

47. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

48. 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

[10] 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).

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

[12] *Id.*

records can go from $20 say up to—we've even seen $60 or $70."[13] 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.[14]

49. 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,

[13] 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.

[14] 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.

> found it hard to get hired for a job, or even been fired by their employers.[15]

50. 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.**"[16]

51. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [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."[17]

52. Even if stolen Private Information 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

---

[15] 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/.

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

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

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.

B. Defendant Medibase Breached Its Duty to Protect Plaintiff and Class Members' Private Information.

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

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

55. On or around January 26, 2024, Defendant Medibase became aware of a ransomware attack on its system.

56. The Data Breach occurred as a direct result of Defendant Medibase's failure to implement and follow basic security procedures, and its failure to follow

its own policies, in order to protect Plaintiff and Class Members' Private Information.

57. On July 5, 2024, Defendant Medibase sent Plaintiff and Class Members Notice Letters about their involvement in the Breach.[18]

C. Plaintiff and Class Members Suffered Damages.

58. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

59. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of

[18] *See* ***Exhibit A***.

Defendants' conduct. Further, the value of Plaintiff and Class Members' Private Information has been diminished by its exposure in the Data Breach.

60. As a result of Defendants' failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of Private Information.

61. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[19]

62. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[20]

63. "Actors buying and selling Private Information from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[21]

[19]https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.
[20]https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.
[21] *Id.*

64. The reality is that cybercriminals seek nefarious outcomes from a data breach" and "stolen health data can be used to carry out a variety of crimes."[22]

65. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[23]

66. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[24]

67. Plaintiff and Class Members have also been injured by Defendants' unauthorized disclosure of their confidential and private medical records and PHI.

68. Plaintiff and Class Members are also at a continued risk because their information remains in Defendants' systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect Plaintiff and Class Members' Private Information.

COMMON INJURIES AND DAMAGES

[22]https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[23] *Id.*
[24]https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

69. As result of Defendants' ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

70. 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 Plaintiff and Class Members has materialized and is imminent, and Plaintiff 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 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 Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and Class Members' Private Information.

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

71. 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.

72. 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.

73. 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.

74. The dark web is an unindexed layer of the Internet that requires special

software or authentication to access.[25] 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.[26] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

75. 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.[27] 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

[25] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[26] *Id.*
[27] *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.

Security numbers, dates of birth, and medical information.[28] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[29]

76. 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.[30]

77. 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

---

[28] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[29] *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.
[30] Social Security Administration, *Identity Theft and Your Social Security number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

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.

78. 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."[31]

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

[31] 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.

for additional credit lines.[32]

80. 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."[33]

81. 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

82. The development of "Fullz" packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff 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

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

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

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

83. 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.[34]

84. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[35] Defendants did not rapidly report to Plaintiff and the Class that their Private Information had been stolen.

85. 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.

86. 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

[34] *See* https://www.fbi.gov/news/stories/2019-Internet-crime-report-released-021120.
[35] *Id.*

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.

87. 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, Plaintiff and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

88. 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."[36]

89. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted

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

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.[37]

90. 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 protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[38]

91. Defendants' failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff and Class Members' injury by depriving them

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

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

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.

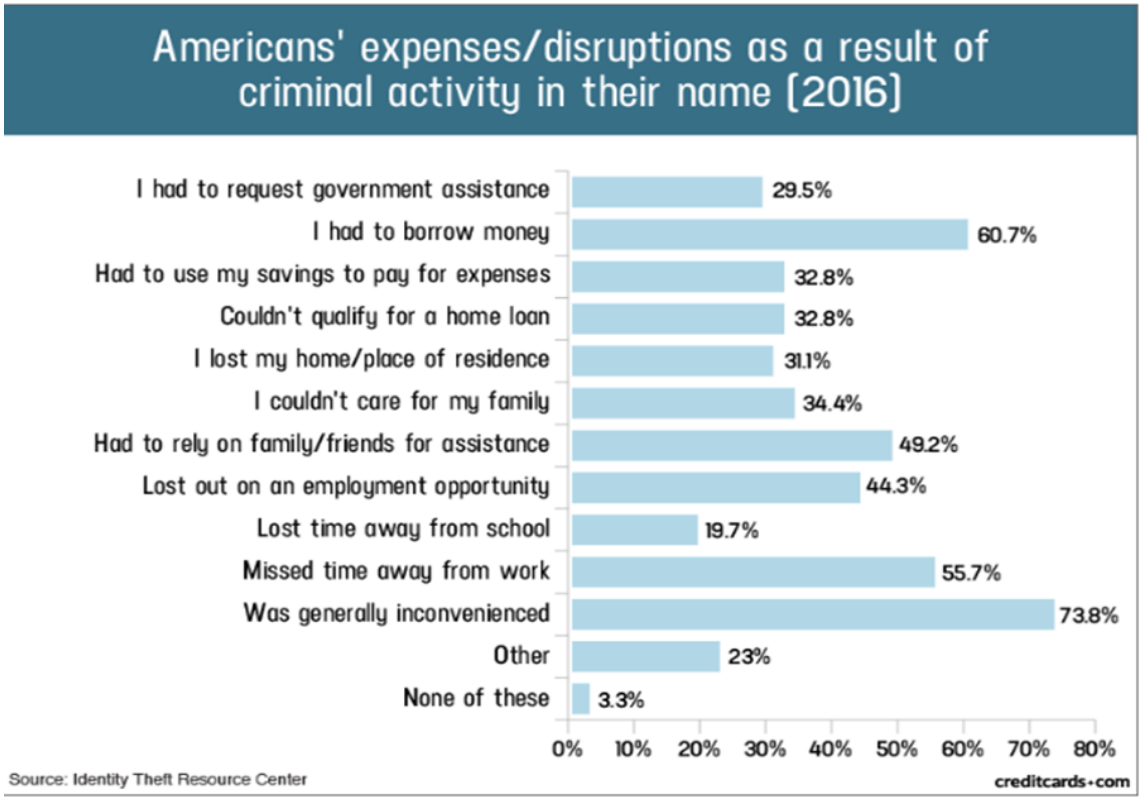
B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

92. 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.

93. Plaintiff 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.

94. A study by Identity Theft Resource Center shows the multitude of

harms caused by fraudulent use of personal and financial information:[39]



95. In the event that Plaintiff 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."[40] Indeed, the FTC recommends that identity theft

[39] "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.

[40] *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").

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 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.[41]

C. Diminution of Value of the Private Information

96. Private Information is a valuable property right.[42] 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.

97. 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.

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

[42] *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).

Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

98. Private Information can sell for as much as $363 per record according to the Infosec Institute.[43]

99. 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.[44]

100. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[45] 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.[46, 47] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[48]

---

[43] *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/.

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

[45] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[46] https://datacoup.com/.

[47] https://digi.me/what-is-digime/.

[48] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

101. As a result of the Data Breach, Plaintiff 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.

102. To date, Defendants have done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendants offered free credit monitoring as a solution to the Data Breach.

103. Defendants also place the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for credit services, as opposed to automatically enrolling all victims of this Data Breach.

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

claims.

105. 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.

106. 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.[49] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

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

108. 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 Defendants

[49] *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.

Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendants failure to safeguard their Private Information.

E. Injunctive Relief is Necessary to Protect Against Future Data Breaches.

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

110. Because of Defendants' failure to prevent the Data Breach, Plaintiff 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 Defendants fail to take appropriate measures to protect the Private Information.

G. Lack of Compensation

111. Plaintiff 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.

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

113. Further, Plaintiff 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. Plaintiff 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.

114. 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.

115. In addition, Plaintiff 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.

116. Plaintiff 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.

117. Defendants' delay in identifying and 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, Defendants knew of the breach and

failed to timely notify all victims. They have yet to offer an explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiff(s) and Class.

CLASS ALLEGATIONS

118. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States whose Private Information was compromised in the Defendants' Data Breach.

119. Excluded from the Class are Defendants, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendants have 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.

120. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

121. **Numerosity.** The class described above is 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. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendants' records, including but not limited to, the files implicated in the Data Breach.

122. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendants had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendants had a duty to maintain the confidentiality of Plaintiff and Class Members' Private Information;

c. Whether Defendants breached their obligations to maintain Plaintiff and the Class Members' medical information in confidence;

d. Whether Defendants were negligent in collecting, storing and safeguarding Plaintiff and Class Members' Private Information, and breached their duties thereby;

e. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct;

f. Whether Plaintiff and Class Members are entitled to restitution or disgorgement as a result of Defendants' wrongful conduct; and

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

123. **Typicality**. Plaintiff's claims are typical of the claims of the Class Members. The claims of the Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendants to safeguard Private Information. Plaintiff and Class Members' information was stored by Defendants' software, each having their Private Information obtained by an unauthorized third party.

124. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class Members she seek to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's 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 Plaintiff and Plaintiff's counsel.

125. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their common law and statutory duties to secure Private Information on their network server, then Plaintiff and each Class Member

suffered damages from the exposure of sensitive Private Information in the Data Breach.

126. **Superiority.** 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.

127. **Manageability.** The precise size of the Class is unknown without the disclosure of Defendants' records. The claims of Plaintiff 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 Plaintiff and the Class.

FIRST CAUSE OF ACTION
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

128. Plaintiff restates and realleges the allegations in paragraphs 1 through 127 above as if fully set forth herein.

129. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information and keep it from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

130. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

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

132. Defendants breached their duties owed to Plaintiff and Class Members and thus were negligent. Defendants breached these duties by, among other things: (a) mismanaging their systems 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 their 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 their 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 their own policies and practices published to its clients.

133. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, the Private Information would not have been compromised.

134. 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 Defendants or failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendants' duty.

135. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of a data breach involving the Private Information of their customers.

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

137. Defendants' violation of Section 5 of the FTC Act constitutes negligence per se.

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

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

140. As a direct and proximate result of Defendants' negligence, Plaintiff 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 Defendants 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 Defendants with the mutual understanding that Defendants would safeguard Plaintiff 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 Defendants possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and Class Members' data;

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

j. The erosion of the essential and confidential relationship between Staten Island University Hospital—as healthcare provider—and Plaintiff and Class Members as patients; and

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

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

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class against Defendant Staten Island University Hospital)

142. Plaintiff restates and realleges the allegations in paragraphs 1 through 127 above as if fully set forth herein.

143. This count is brought against Staten Island University Hospital (for purposes of this count "Defendant").

144. When Plaintiff and Class Members provided their personal information to Defendant, Plaintiff and Class Members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their data had been breached and compromised.

145. Defendant required Plaintiff and Class Members to provide and entrust their PHI and PII as a condition of obtaining Defendant's services.

146. Plaintiff and Class Members would not have provided and entrusted their PHI and PII to Defendant in the absence of the implied contract between them and Defendant.

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

148. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the personal information of Plaintiff and Class Members and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach.

149. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff 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.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class against Defendant State Island University Hospital)

150. Plaintiff restates and realleges paragraphs 1 to 127 as if fully set forth herein.

151. This count is brought against Staten Island University Hospital (for purposes of this count "Defendant").

152. Plaintiff brings this claim in the alternative to her breach of implied contract claim above.

153. Plaintiff and Class Members conferred a benefit on Defendant by way of paying Defendant for healthcare services.

154. The monies paid to Defendant was supposed to be used by Defendants, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class Members.

155. Defendant failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class Members, and as a result Defendant was overpaid.

156. Under principles of equity and good conscience, Defendant should not be permitted to retain the money because Defendant failed to provide adequate safeguards and security measures to protect Plaintiff and Class Members' Private Information that they paid for but did not receive.

157. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

158. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

159. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and

other compensation obtained by Defendants, plus attorneys' fees, costs, and interest thereon.

FOURTH CAUSE OF ACTION
BREACH OF THIRD PARTY BENFICIARY CONTRACT
(On Behalf of Plaintiff and the Class against Medibase)

160. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 127, as if fully set forth herein.

161. This count is brought against Medibase (for purposes of this count "Defendant").

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

163. Such contracts were made expressly for the benefit of Plaintiff 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 Plaintiff and the Class was the direct and primary objective of the contracting parties, and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

164. Defendant knew that if it were to breach these contracts with its clients, Plaintiff and the Class would be harmed.

165. Defendant breached its contracts with its clients and, as a result, Plaintiff 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.

166. As foreseen, Plaintiff 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.

167. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

FIFTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class against Medibase)

168. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 127, as if fully set forth herein.

169. This count is brought against Medibase (for purposes of this count "Defendant").

170. Plaintiff brings this claim in the alternative to her breach of third-party beneficiary contract claim above.

171. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Defendant should have provided adequate data security for Plaintiff and Class Members.

172. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form their Private Information as a necessary part of their receiving healthcare services at Defendant's clients. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

173. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

174. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

175. Defendant, however, failed to secure Plaintiff and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

176. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

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

178. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

179. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

180. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

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

182. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (xi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

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

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

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, on behalf of herself and Class Members, requests judgment against Defendants and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

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

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the

interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and securing checks;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvi. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class,

and to report any deficiencies with compliance of the Court's final judgment;

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

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees pursuant to O.C.G.A. Section 13-6-11, and as otherwise allowed by law;

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

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

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: July 12, 2024

Respectfully submitted,

By: */s/ MaryBeth V. Gibson*
MaryBeth V. Gibson
GA Bar No. 725843
Gibson Consumer Law Group, LLC
4279 Roswell Road
Suite 208-108
Atlanta, GA 30342
Telephone: (678) 642-2503
marybeth@gibsonconsumerlawgroup.com

Jeff Ostrow*

KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
E: ostrow@kolawyers.com

*application for admission *pro hac vice* forthcoming

Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF COMPLIANCE

I certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

Dated: July 12, 2024

By: /s/ MaryBeth V. Gibson
MaryBeth V. Gibson

ClassAction.org
