UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

MULHAM HAFIEZ, GABRIELLE CROWLEY, LAURA FASOLO, LEIGH TILLER, and BENNY GREENE, individually and on behalf of all others similarly situated, Plaintiffs, v. THE HILB GROUP OPERATING COMPANY, LLC, Defendant.	Lead Civil Action No.: 3:23-cv-759-JAB **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Mulham Hafiez, Gabrielle Crowley, Laura Fasolo, Leigh Tiller, and Benny Greene, individually, and on behalf of all others similarly situated, bring this Consolidated Amended Class Action Complaint ("Complaint") against Defendant The Hilb Group Operating Company, LLC ("Hilb" or "Defendant"), for its failure to properly secure and safeguard Plaintiffs' and Class Members' personally identifiable information ("PII") stored within Defendant's information network. Plaintiffs seek to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations on information and belief, except as to their own actions, which are made on personal knowledge, the investigation of their counsel, and the facts that are a matter of public record.

INTRODUCTION

1. This class action arises out of the targeted cyberattack and data breach ("Data Breach") on Hilb's network that resulted in unauthorized access to highly sensitive data. As a result of the Data Breach, Plaintiffs and at least 81,539 other similarly situated persons suffered

actual misuse of their data, ascertainable losses, and are subject to the present and continuing risk of imminent harm caused by the compromise of their sensitive personal information.

2. Defendant is an insurance agency with over 125 branches that offers insurance and other products and services to its clients and/or customers.[1]

3. Defendant acquired, collected, and stored Plaintiffs' and Class Members' PII, and stored that Private Information, unencrypted, in an Internet-accessible environment on Hilb's network.

4. At all relevant times, Defendant knew or should have known that Plaintiffs and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PII.

5. A massive and preventable cyberattack occurred between December 1, 2022, and January 12, 2023. On no later than December 1, 2022, upon information and belief, unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' PII as hosted with Defendant, with the intent of engaging in the misuse of the PII, including marketing and selling of Plaintiffs' and Class Members' PII.

6. In this cyberattack, cybercriminals infiltrated Defendant's inadequately protected email account servers and accessed and exfiltrated highly sensitive Private Information belonging to Plaintiffs and Class Members which was being kept unprotected (the "Data Breach").

7. The specific information that was targeted, compromised, and exfiltrated in the Data Breach includes full names, Social Security numbers, financial account numbers in combination with security codes, access codes, password and/or PINs (collectively "PII"), Health

[1] https://www.hilbgroup.com/ (last accessed March 4, 2024).

Insurance Information, and Medical Information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

8. Plaintiffs' and Class Members' Private Information—which was entrusted to Defendant, its officials, and agents—was targeted, compromised, and unlawfully accessed due to the Data Breach and Defendant admits that this information was "compromised" from its network during the Data Breach.

9. PII generally incorporates information that can be used to distinguish or trace an individual's identity, and is generally defined to include certain identifiers that do not on their face name an individual, but that is considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

10. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of his and Class Members' Private Information that Defendant collected and maintained.

11. Defendant maintained the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack 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 the Private Information from those risks left that property in a dangerous condition.

12. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally,

willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

13. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiffs and Class Members in the future.

14. Upon information and belief, Defendant and its employees additionally failed to properly monitor the computer networks, IT systems, and integrated services that housed Plaintiffs' and Class Members' Private Information.

15. The cyberattack perpetrated against Defendant was targeted at acquiring the Private Information stored by Defendant due to its value on internet black markets where it is offered for sale to identity thieves and fraudsters.

16. As a result of Defendant's negligent conduct, Plaintiffs' and Class Members' identities are now at risk because the Private Information that Defendant collected and maintained is now in the hands of malicious cybercriminals. The risks to Plaintiffs and Class Members will remain for their respective lifetimes.

17. Defendant also failed to provide timely and adequate notice to Plaintiffs and other Class Members that their Private Information had been subject to the unauthorized access by an unknown, unauthorized party. While the Data Breach began December 1, 2022, Defendant did not begin informing victims of the Data Breach until November 2, 2023, over 11 months later.

18. Indeed, Plaintiffs and Class Members were wholly unaware of the Data Breach

until they received Notice Letters[2] from Defendant. During this time, Plaintiffs and Class Members were unaware that their sensitive Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

19. Defendant chose not to notify affected customers or, upon information and belief, anyone of the Data Breach, instead choosing to address the incident in-house by implementing other purported safeguards to some aspects of its computer security.

20. The Notice Letter provides no further information regarding the Data Breach and only recommends how victims can place a fraud alert or credit freeze on their account and how to sign up for the limited identity monitoring services Defendant offered in response to the Data Breach. The Notice Letter does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or most importantly, whether Plaintiffs' and Class Members' Private Information remains in the possession of criminals.

21. Currently, the full extent of the types of Private Information, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

22. Hilb's Notice Letter admitted that the Private Information accessed included individuals' full names, Social Security numbers, health insurance information, and other sensitive information.

---

[2] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/efcbb550-4093-4bdf-95a0-ecd868472099.shtml (last accessed March 4, 2024).

23. Through its Notice Letter, Hilb also recognized the actual imminent harm and injury that flowed from the Data Breach, encouraging breach victims to take steps to mitigate their risk of identity theft, including reviewing financial accounts and credit reports for possible fraud.

24. Hilb has offered abbreviated, non-automatic, single-bureau credit monitoring services to victims thereby identifying the harm posed to Plaintiffs and Class Members because of the Data Breach, which does not adequately address the lifelong harm that victims face following the Data Breach. Indeed, the Data Breach involves Private Information that cannot be changed, such as Social Security numbers.

25. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

26. As a result of the targeted Data Breach, Plaintiffs and Class Members have been exposed to a present and continuing risk of fraud and identity theft. Plaintiffs and Class Members must now closely monitor their financial accounts to guard against identity theft for the rest of their lives.

27. Plaintiffs and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

28. By their 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.

29. Accordingly, Plaintiffs bring claims on behalf of themselves and the Classes for: (i) negligence; (ii) breach of implied contract; (iii) breach of implied covenant of good faith and fair dealing; (iv) unjust enrichment; and (v) declaratory judgment and injunctive relief.

30. Plaintiffs and Class Members have a continued interest in ensuring that their information is and remains safe, and they are thus entitled to injunctive and other equitable relief.

31. Through these claims, Plaintiffs seek, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems and integrated services, future annual audits, and adequate credit monitoring services.

PARTIES

32. Plaintiff Mulham Hafiez is an adult individual and citizen of Virginia. He resides in Henrico, where he intends to remain for the foreseeable future.

33. Plaintiff Hafiez received a notice letter from Defendant Hilb dated November 2, 2023, informing him of the Data Breach and the exposure of his Private Information.

34. Plaintiff Hafiez was not familiar with Defendant prior to receiving the Notice Letter in the mail, but, upon information and belief, Plaintiff, directly or indirectly provided his information to The Hilb Group Operating Company LLC in the past.

35. The notice letter informed Plaintiff Hafiez that his full name and health insurance information was potentially compromised in the Data Breach.

36. Plaintiff Gabrielle Crowley is an adult individual and citizen of New York. She resides in New York County, where she intends to remain for the foreseeable future.

37. Plaintiff Crowley received a notice letter from Defendant Hilb dated November 2, 2023, informing her of the Data Breach and the exposure of her Private Information.

38. Plaintiff Crowley was not familiar with Defendant prior to receiving the Notice Letter in the mail, but, upon information and belief, Plaintiff, directly or indirectly provided her information to The Hilb Group Operating Company LLC in the past.

39. The notice letter informed Plaintiff Crowley that her first and last name, health insurance information, medical information, and Social Security number was potentially compromised in the Data Breach.

40. Plaintiff Laura Fasolo is an adult individual and citizen of New Jersey. She resides in Essex County, where she intends to remain for the foreseeable future.

41. Plaintiff Fasolo received a notice letter from Defendant Hilb dated November 2, 2023, informing her of the Data Breach and the exposure of her Private Information.

42. Plaintiff Fasolo was not familiar with Defendant prior to receiving the Notice Letter in the mail, but, upon information and belief, Plaintiff, directly or indirectly provided her information to The Hilb Group Operating Company LLC in the past.

43. The notice letter informed Plaintiff Fasolo that her first and last name, health insurance information, and Social Security number was potentially compromised in the Data Breach.

44. Plaintiff Leigh Tiller is an adult individual and citizen of West Virginia. She resides in Kanawha County, where she intends to remain for the foreseeable future.

45. Plaintiff Tiller received a notice letter from Defendant Hilb dated November 2, 2023, informing her of the Data Breach and the exposure of her Private Information.

46. Plaintiff Tiller provided her information to The Hilb Group Operating Company

LLC indirectly through her previous employer, Ciox.

47. The notice letter informed Plaintiff Tiller that her full name and social security number was potentially compromised in the Data Breach.

48. Plaintiff Benny Greene is an adult individual and citizen of Tennessee. He resides in Carter County, where he intends to remain for the foreseeable future.

49. Plaintiff Greene received a notice letter from Defendant Hilb dated November 2, 2023, informing him of the Data Breach and the exposure of his Private Information.

50. Plaintiff Greene was not familiar with Defendant prior to receiving the Notice Letter in the mail but, upon information and belief, Plaintiff Greene directly or indirectly provided his information to The Hilb Group Operating Company LLC in the past.

51. The notice letter informed Plaintiff Greene that his full name and social security number was potentially compromised in the Data Breach.

52. Defendant The Hilb Group Operating Company, LLC is a Delaware limited liability company with its principal place of business located at 6802 Paragon Place, Suite 200, Richmond Virginia 23230.

53. Upon information and belief, The Hilb Group Operating Company LLC has at least one member, R. Judson Elliott, Jr., who is a resident and citizen of Virginia. R. Judson Elliott, Jr., is listed as one of the founding members of the Hilb Group leadership team on The Hilb Group website.[3] Additionally, R. Judson Elliott, Jr., lists himself as a "founding partner/Executive Vice President" of The Hilb Group, LLC, on his personal LinkedIn page.[4]

JURISDICTION AND VENUE

[3] https://www.hilbgroup.com/about-us/ (last visited March 4, 2024).
[4] https://www.linkedin.com/in/jud-elliott-a204b11a/ (last visited March 4, 2024).

54. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class are citizens of a different state than Defendant,[5] there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

55. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in this District, Defendant conducts substantial business in Virginia and this District through its headquarters, offices, parents, and affiliates, and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

56. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal places of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

A. Defendant's Business

57. Defendant Hilb is an insurance brokerage and advisory firm headquartered in Richmond, Virginia, with 1,500 employees and 100+ agency locations in more than 20 states. Hilb provides services to all 50 states.[6]

58. As a condition of obtaining insurance or other products and/or services at Hilb, Defendant requires its customers and clients' employees to provide Hilb with sensitive and confidential Private Information, including their names, Social Security numbers, and other

[5] According to the report submitted to the Office of the Maine Attorney General, 105 Maine residents were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/efcbb550-4093-4bdf-95a0-ecd868472099.shtml (last visited March 4, 2024).

[6] https://hilbgroupmedicare.com/about-us/ (last visited March 4, 2024).

sensitive information.

59. The information held by Defendant in its computer systems included the unencrypted Private Information of Plaintiffs and Class Members.

60. Upon information and belief, Defendant made promises and representations to its customers' and clients' employees—including Class Members—that the Private Information collected from them as a condition of obtaining insurance or other products and/or services at Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

61. Indeed, Defendant's Privacy Policy provides that: "[w]e implement technical, organizational, administrative and physical measures to help ensure a level of security appropriate to the risk to the personal information we collect, use, disclose and process. These measures are aimed at ensuring the on-going integrity and confidentiality of personal information. We evaluate these measures on a regular basis to help ensure the security of the processing."[7]

62. Moreover, Hilb markets itself to its clients as a cybersecurity expert, stating that: "[l]icensed insurance professionals at Hilb Group will help you to address the multitude of new cyber risks, reduce risk when sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual, and to acquire affordable insurance protection."[8]

63. Plaintiffs and Class Members provided their Private Information, directly or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant

[7] https://www.hilbgroup.com/privacy-policy/ (last accessed March 4, 2024).
[8] https://www.hilbgroup.com/commercial-lines/cyber-risk/ (last accessed March 4, 2024).

would comply with its obligations to keep such information confidential and secure from unauthorized access.

64. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

65. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties and to ensure that third parties with whom it shared Private Information would do the same. Defendant has a legal duty to keep consumer's Private Information safe and confidential.

66. Defendant had obligations created by FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

67. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

68. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

B. The Cyberattack

69. On or about November 2, 2023, Defendant began sending Plaintiffs and other Data Breach victims an untitled letter (the "Notice Letter"), informing them, in relevant part, that:

> **What Happened:** On or about January 10, 2023, we discovered suspicious activity related to several employee email accounts. Upon discovery, we took immediate action to address and investigate the event, which included engaging third-party specialists to assist with determining the nature and scope of the event. A thorough investigation determined that an unauthorized actor gained access to employee email accounts for a limited period of time between December 1, 2022 and January 12, 2023. We then began a thorough review of the contents of the email accounts in order to determine the type(s) of information contained within the accounts and to whom that information related. On July 28, 2023, this review was completed, and we immediately began working to locate address information. On October 9, 2023, we completed an address review and we worked to provide potentially impacted individuals with this notification.
>
> **What Information Was Involved:** The types of information that may have been contained within the email account includes your first and last name, in combination with the following date element(s): Health Insurance Information.[9]

70. Omitted from the Notice Letter was any explanation as to why Defendant failed to inform Plaintiffs and Class Members of the Data Breach's occurrence for *nearly ten months* after detecting the cyberattack, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

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

72. Defendant did not use reasonable security procedures and practices appropriate to

[9] The Notice Letter.

the nature of the sensitive information they collected from Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

73. As a result, the attacker accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members, including Social Security numbers for some Class Members.[10] Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

74. Plaintiffs further believe that their Private Information and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

C. Defendant Acquires, Collects, and Stores Consumers' Private Information

75. As a condition to obtain insurance and/or other products or services from Hilb, Plaintiffs and Class Members were required to give their sensitive and confidential Private Information, directly or indirectly, to Defendant.

76. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiffs' and Class Members' Private Information, Defendant would be unable to perform its services.

77. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

78. Plaintiffs and Class Members have taken reasonable steps to maintain the

[10] The Notice Letter.

confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

79. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

80. Upon information and belief, Defendant made promises to Plaintiffs and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

81. Defendant's Privacy Policy, posted on its website, states that "The Hilb Group, LLC is committed to respecting personal privacy, and safeguarding individual record confidentiality and system security."[11]

82. Defendant's Privacy Policy states that it shares customers' Private Information with including service and business providers, its affiliates, law enforcement, courts, regulators, and asset purchasers.[12] Defendant's Privacy Policy does not say that Defendant shares Private Information with unauthorized cyber-criminals.

83. Defendant's Privacy Policy further provides that: "[w]e implement technical, organizational, administrative and physical measures to help ensure a level of security appropriate to the risk to the personal information we collect, use, disclose and process. These measures are aimed at ensuring the on-going integrity and confidentiality of personal information. We evaluate

---

[11] *Privacy Policy*, https://www.hilbgroup.com/privacy policy/#:~:text=We%20may%20share%20your%20personal%20information%20with%20other%20The%20Hilb,described%20in%20this%20privacy%20notice (last visited March 4, 2024).
[12] *Id.*

these measures on a regular basis to help ensure the security of the processing."[13]

84. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

D. The Data Breach was a Foreseeable Risk of which Defendant was on Notice

85. As a large national business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which Hilb was aware and knew it had a duty to guard against. It is well-known that insurance businesses such as Defendant, which collect and store the confidential and sensitive PII of thousands of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

86. The targeted cyberattack against Defendant was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of customers, like Plaintiffs and Class Members.

87. Data thieves regularly target companies like Defendant due to the highly sensitive information that it uses in its regular business. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

88. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting insurance companies that

[13] *Id.*

collect and store Private Information and other sensitive information, like Defendant, preceding the date of the breach.

89. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[14]

90. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

91. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

92. Additionally, as companies became more dependent on computer systems to run their business,[15] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[16]

93. Defendant was—or should have been—fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting more than eighty thousand individuals' Private Information,[17] and, thus, the significant number of individuals who would be

---

[14] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last visited March 4, 2024).

[15] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited March 4, 2024).

[16] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited March 4, 2024).

[17] According to the report submitted to the Office of the Maine Attorney General, 81,539 persons were impacted in the Data Breach. *See*

harmed by the exposure of the unencrypted data.

94. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to address the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' Private Information. Moreover, once this service expires, Plaintiffs and Class Members will be forced to incur out of pocket expenses for necessary identity monitoring services.

95. Defendant's offer of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

96. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

97. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue indefinitely.

98. As an insurance company in possession of its customers' and clients' employees' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiffs and Class Members and of the foreseeable

---

https://apps.web.maine.gov/online/aeviewer/ME/40/efcbb550-4093-4bdf-95a0-ecd868472099.shtml (last visited March 4, 2024).

consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

E. The Value of Personally Identifiable Information.

99. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] The FTC describes "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."[19]

100. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[20]

101. For example, Personal Information can be sold at a price ranging from $40 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

102. For example, Social Security numbers, which Defendant reports was compromised

---

[18] 17 C.F.R. § 248.201 (2013).
[19] *Id.*
[20] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited March 4, 2024).
[21] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited March 4, 2024).
[22] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited March 4, 2024).

in the Data Breach,[23] are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

103. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, 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.[24]

104. 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.

105. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[25]

---

[23] https://apps.web.maine.gov/online/aeviewer/ME/40/efcbb550-4093-4bdf-95a0-ecd868472099.shtml (last visited March 4, 2024).
[24] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited March 4, 2024).
[25] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited March 4, 2024).

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

107. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[26]

108. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, home improvement products and/or services, and housing or even give false information to police.

109. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

---

[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited March 4, 2024).

[27] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited March 4, 2024).

110. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

F. Defendant Fails to Comply with FTC Guidelines

111. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

112. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[28] 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.[29]

113. The FTC further 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

[28] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 4, 2024).
[29] *Id*.

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

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

115. These FTC enforcement actions include actions against insurance companies, like Defendant.

116. Defendant failed to properly implement basic data security practices.

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

118. Defendant was at all times fully aware of their obligation to protect the Private Information of the individuals in its network. Defendant was also aware of the significant repercussions that would result from their failure to do so.

G. Defendant Fails to Comply with HIPAA

119. Defendant is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

120. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

121. HIPAA's Security Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

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

123. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to maintain the confidentiality and integrity of electronic PHI that is creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. §164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

d. Failing to comply with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. §164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308; and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. §164.530(c).

H. Defendant Fails to Comply with Industry Standards

124. As shown above, experts studying cyber security routinely identify insurance companies as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

125. Several best practices have been identified that at a minimum should be implemented by insurance companies, like Defendant, including but not limited to: educating all

employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

126. Other best cybersecurity practices that are standard in the insurance industry include: installing appropriate malware detection software; monitoring and limiting the 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; training staff regarding critical points.

127. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

128. These foregoing frameworks are existing and applicable industry standards in the insurance industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

I. Defendant's Breach

129. Hilb breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because Hilb failed to ensure that the information it shared with its affiliates was properly encrypted while in transit and that its partners used data security practices appropriate to the nature of information being shared on their computer systems and network. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect Private Information;

c. Failing to ensure that its vendors with access to their computer systems and data employed reasonable security procedures;

d. Failing to ensure the confidentiality and integrity of electronic Private Information it created, received, maintained, and/or transmitted;

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software programs that have been granted access rights;

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

g. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

h. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic Private Information;

i. Failing to train all members of its workforce effectively on the policies and procedures regarding Private Information;

j. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

k. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

l. Failing to adhere to industry standards for cybersecurity as discussed above; and,

m. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

130. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Defendant's online insurance application flow, which provided unauthorized actors with unsecured and unencrypted Private Information.

131. Accordingly, as outlined below, Plaintiffs and Class Members now face a present, increased risk of fraud and identity theft.

J. Common Injuries and Damages

132. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with meaningful relief for the damages they have suffered as a result of the Data Breach.

133. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) 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.

The Data Breach Increases the Risk of Identity Theft for the Plaintiffs and the Class

134. The unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

135. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

136. 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.

137. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

138. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[30]

[30] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone

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

140. The development of "Fullz" packages means here that the stolen Private Information 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 Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

141. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and Class Members.

142. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

143. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

---

with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited March 4, 2024).

144. 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, a 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.

145. Thus, due to the actual and imminent risk of identity theft, Defendant's Notice Letter instructs Plaintiffs and Class Members to do the following:

> We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided addition information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, including activating the complimentary credit monitoring and identity protection services we are offering.[31]

146. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter as well as monitoring their financial accounts for unauthorized activity, which may take years to discover and detect.

147. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[32]

---

[31] The Notice Letter.

[32] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full

148. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven 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.[33]

Diminution of Value of Private Information

149. PII and PHI are valuable property rights.[34] Their value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

150. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[35]

151. An active and robust legitimate marketplace for PII also exists. In 2019, the data

---

Extent Is Unknown (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited March 4, 2024).

[33] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited March 4, 2024).

[34] *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 (last visited March 4, 2024) ("GAO Report").

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

brokering industry was worth roughly $200 billion.[36]

152. 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.[37,38] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[39]

153. Theft of PHI is also 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]

154. Medical data sells for $1,000 and up on the Dark Web.[41]

155. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[42]

---

[36] *See* Ashiq Ja, *Hackers Selling Financial Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-financial-data-in-the-black-market/ (last visited March 4, 2024).
[37] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited March 4, 2024).
[38] https://datacoup.com/ (last visited March 4, 2024).
[39] https://digi.me/what-is-digime/ (last visited March 4, 2024).
[40] *Medical I.D. Theft*, EFraudPrevention, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited March 4, 2024).
[41] David Lukic, *What is Your Personal Information Worth on the Dark Web*, ID Strong (Aug. 20, 2021), https://www.idstrong.com/sentinel/how-much-is-your-data-worth-on-the-dark-web/ (last visited March 4, 2024).
[42] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited March 4, 2024).

156. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[43] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[44]

157. 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 by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

158. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

159. The fraudulent activity resulting from the Data Breach may not come to light for years.

---

[43] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited March 4, 2024).

[44] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/ (last visited March 4, 2024).

160. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

161. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to more than eighty thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

162. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost of Credit & ID Theft Monitoring is Reasonable & Necessary

163. Given the type of targeted attack in this case, the sophisticated criminal activity, the sensitive type of Private Information involved in this Data Breach, and the volume of Private Information compromised, 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.

164. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information 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.

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

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

K. Plaintiffs' Experiences

Plaintiff Hafiez's Experience

167. Plaintiff Mulham Hafiez is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Hafiez stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Hafiez diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff Hafiez uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

168. Plaintiff Hafiez only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff Hafiez's Private Information was within the possession and control of Defendant at the time of the Data Breach.

169. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Hafiez suffered injury from a loss of privacy.

170. Plaintiff Hafiez has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff Hafiez entrusted to Defendant. This information has inherent value that Plaintiff Hafiez was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

171. The Data Breach has also caused Plaintiff Hafiez to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

172. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff Hafiez signed up for the credit monitoring and identity theft protection services offered by Defendant.

173. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Hafiez to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his financial accounts to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

174. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Hafiez to suffer stress, fear, and anxiety.

175. Plaintiff Hafiez has a continuing interest in ensuring that Plaintiff Hafiez's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Crowley's Experience

176. Plaintiff Crowley is a reasonably cautious person and is therefore careful about

sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Crowley diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her Plaintiff Crowley uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

177. Plaintiff Crowley only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff Crowley's Private Information was within the possession and control of Defendant at the time of the Data Breach.

178. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Crowley suffered injury from a loss of privacy.

179. Plaintiff Crowley has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Crowley entrusted to Defendant. This information has inherent value that Plaintiff Crowley was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

180. Upon information and belief, Plaintiff Crowley's Private Information has already been stolen and misused.

181. Specifically, in February of 2024, Plaintiff Crowley received an email from an unknown address informing her that her Private Information was found on the dark web. Further,

on March 1, 2024, Plaintiff Crowley purchased a dark web report through G-Mail Security. The report alerted her that her Private Information, such as her name, address, email, and phone number, had been discovered on the dark web starting January 5, 2023.

182. Next, on September 5, 2023 and January 6, 2024, Plaintiff Crowley received a confirmation email from Facebook that a request was made to change her password. Plaintiff Crowley never attempted to change her Facebook password. Finally, on February 7, 2024 and February 16, 2024, Plaintiff Crowley received multiple invoices in her name from PayPal and Norton LifeLock for the purchase of products that she has never purchased. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Crowley's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

183. Furthermore, Plaintiff Crowley has experienced a clear increase in spam emails as a result of the Data Breach.

184. The Data Breach has also caused Plaintiff Crowley to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

185. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Crowley has lost approximately seven (7) hours related to efforts to mitigate or investigate the breach, including calling the phone number listed on the breach letter, requesting and monitoring her credit reports, and purchasing dark web reports.

186. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Crowley to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time,

which has been lost forever and cannot be recaptured, was spent at the Defendant's direction.

187. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Crowley to suffer stress, fear, and anxiety.

188. Plaintiff Crowley has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Fasolo's Experience

189. Plaintiff Fasolo is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Fasolo stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Fasolo diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be. When it is available to her, Plaintiff Fasolo uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

190. Plaintiff Fasolo only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff Fasolo's Private Information was within the possession and control of Defendant at the time of the Data Breach.

191. In the instant that Plaintiff Fasolo's Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Fasolo suffered injury from a loss

of privacy.

192. Plaintiff Fasolo has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Fasolo entrusted to Defendant. This information has inherent value that Plaintiff Fasolo was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

193. Upon information and belief, Plaintiff Fasolo's Private Information has already been stolen and misused as she experienced incidents of fraud and identity theft so far in the form of unauthorized transactions and the opening of a Bank of America account in her name. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Fasolo's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

194. Specifically, on May 18, 2023, Plaintiff Fasolo received a letter from Bank of America informing her of the decision to close an account opened in her name because Bank of America was unable to verify her identity. Plaintiff Fasolo was completely unaware this account was opened in her name and at no time did Plaintiff Fasolo attempt to open a new account with Bank of America.

195. Further, between October 4, 2023 through October 5, 2023, a total of $4,831.00 was withdrawn from Plaintiff Fasolo's Bank of America account through no action of her own to an unknown recipient. On October 10, 2023, the account was closed without Plaintiff's consent and $150.00 was withdrawn as an "account closing transaction".

196. Plaintiff Fasolo has also experienced a clear increase in spam calls as a result of the Data Breach.

197. The Data Breach has also caused Plaintiff Fasolo to suffer imminent and impending

injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

198. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff Fasolo has spent hours, speaking with her financial institution, credit reporting agencies, requesting/monitoring credit reports, and researching and signing up for credit monitoring services.

199. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Fasolo to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at the Defendant's direction.

200. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Fasolo to suffer stress, fear, and anxiety.

201. Plaintiff Fasolo has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Tiller's Experience

202. Plaintiff Tiller is a reasonably cautious person and is therefore careful about sharing her sensitive Private Information. As a result, she has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as

protected as it can be. When it is available to her Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to her Private Information.

203. Plaintiff Tiller only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

204. In the instant that her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

205. Plaintiff has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

206. Upon information and belief, Plaintiff Tiller's Private Information has already been stolen and misused.

207. Specifically, after the Data Breach, Plaintiff Tiller attempted to open a bank account and was unexpectedly prompted to verify information about a North Dakota address she was unable to recognize. Subsequently, upon reviewing her Credit Karma credit report, she discovered this unknown address linked to a name she did not know. Plaintiff Tiller immediately disputed this entry on her credit report.

208. Furthermore, Plaintiff has experienced a tremendous increase of spam calls and text messages as a result of the Data Breach.

209. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

210. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, and disputing unknown entries made on her credit report. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

211. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

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

Plaintiff Greene's Experience

213. Plaintiff Greene is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be. When it is available to him Plaintiff uses two-factor or multifactor authentication to add an extra layer of security to his Private Information.

214. Plaintiff Greene only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

215. In the instant that his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

216. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database and exfiltrated by cybercriminals.

217. Furthermore, as a result of the Data Breach, Plaintiff has experienced a significant surge in unsolicited spam mail, including numerous credit card offers that he never requested.

218. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

219. As a result of the increased imminent risk of future harm, Plaintiff has spent approximately half an hour every week since the breach self-monitoring his accounts and/or credit reports to ensure no fraudulent activity has occurred.

220. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has

been lost forever and cannot be recaptured, was spent at Defendant's direction.

221. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety as Plaintiff Greene is very concerned that his sensitive Private Information is now in the hands of data thieves and shall remain that way for the remainder of his lifetime and there is nothing Plaintiff Greene can do to retrieve his stolen Private Information from the cyber-criminals.

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

CLASS ACTION ALLEGATIONS

223. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

224. Plaintiffs sue on behalf of themselves and the proposed Class, defined as follows:

> **Nationwide Class**
> **All United States residents who were sent a Notice Letter by Defendant notifying them that their Private Information was actually or potentially accessed or acquired during the Data Breach (the "Class").**

225. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

226. Plaintiffs reserve the right to amend or modify the Class definition and/or add a subclass as this case progresses.

227. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

228. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, according to the report submitted to the Office of the Maine Attorney General, approximately 81,539 persons were impacted in the Data Breach.[45]

229. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

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

b. 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;

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

d. Whether Defendant exercised due diligence in selecting its IT vendors and whether Defendant properly audited or monitored the data security systems of third parties with whom it shared Private Information;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

[45]https://apps.web.maine.gov/online/aeviewer/ME/40/efcbb550-4093-4bdf-95a0-ecd868472099.shtml (last accessed Nov. 8, 2023).

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its vendors' and partners' data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

230. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

231. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect

to the Class as a whole, not on facts or law applicable only to Plaintiffs.

232. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

233. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

234. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

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

236. Likewise, 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 failed to timely notify the public of the Data Breach;

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

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

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and,

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

237. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

COUNT I

Negligence
(On Behalf of Plaintiffs and the Class)

238. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs.

239. Defendant requires its customers and clients' employees to submit non-public Private Information in the ordinary course of providing its insurance services.

240. Plaintiffs and Class Members entrusted Defendant with their Private Information, directly or indirectly, for the purpose of obtaining insurance and/or other products or services from Defendant.

241. Hilb owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

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

243. Hilb had a duty under HIPAA to use reasonable security measures to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

244. Moreover, under HIPAA, Defendant had a duty to render the electronic Private

Information that they maintained as unusable, unreadable, or indecipherable to unauthorized individuals. Specifically, the HIPAA Security Rule requires "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."

245. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Hilb and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Hilb with their confidential Private Information, a necessary part of being customers of Defendant or employees of Defendant's clients.

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

247. Hilb was subject to an "independent duty," untethered to any contract between Hilb and Plaintiffs or the Class.

248. Hilb also had a duty to exercise appropriate clearinghouse practices to remove former customers' and/or employees' Private Information it was no longer required to retain pursuant to regulations.

249. Hilb also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiffs and the Class.

250. Hilb breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Hilb include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former customers' and clients' employees' Private Information it was no longer required to retain pursuant to regulations, and

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

251. Hilb violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein.

252. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

253. Defendant's violation of Section 5 of the FTC Act and other similar state statutes constitutes negligence.

254. Plaintiffs and Class Members are within the class of persons that the FTC Act and other similar state statutes were intended to protect.

255. Defendant's violation of the FTC Act and other similar state statutes is *prima facie* evidence of negligence.

256. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and other similar state statutes were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

257. Plaintiffs and Class Members are within the class of persons that the HIPAA was intended to protect.

258. Defendant violated HIPAA by failing to provide fair, reasonable, or adequate data security to safeguard Plaintiffs' and Class Members' Private Information.

259. The injuries that Defendant inflicted on Plaintiffs and the Class Members are precisely the harms that HIPAA guards against. After all, the Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses which—because of their failure to employ reasonable data security measures for PHI— caused the very same injuries that Defendant inflicted upon Plaintiff and Class Members.

260. Defendant's violation of HIPAA constitutes negligence.

261. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

263. Hilb has full knowledge of the sensitivity of the Private Information and the types

of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

264. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Hilb knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

265. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would result in one or more types of injuries to Plaintiffs and Class Members.

266. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

267. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

268. Hilb had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

269. Hilb admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

270. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and

the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

271. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

272. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class 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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) 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.

273. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

274. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private

Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Hilb fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

275. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

276. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

277. Plaintiffs and Class Members are also entitled to injunctive relief requiring Hilb to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

278. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs.

279. Plaintiffs and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

280. Plaintiffs and the Class were required to—and did—deliver their Private Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

281. Defendant solicited, offered, and invited Class Members to provide their Private

Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

282. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

283. In accepting such information and payment for services, Plaintiffs and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Private Information.

284. In delivering their Private Information to Defendant and providing paying for insurance services and products, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

285. The implied promise of confidentiality included implied promises to take adequate steps to comply with specific industry data security standards, HIPAA, and FTC guidelines on data security.

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

287. Plaintiffs and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

288. Had Defendant disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Private Information to Defendant.

289. Defendant recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

290. Plaintiffs and the other Class Members fully performed their obligations under the implied contracts with Defendant.

291. Defendant breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

292. As a direct and proximate result of Defendant's conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiffs and the Class)

293. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

294. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

295. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

296. Defendant breached the implied covenant of good faith and fair dealing by failing

to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of PII and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

297. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

298. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs.

299. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

300. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving insurance and/or other products or services. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

301. 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 Plaintiffs and Class Members.

302. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs 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.

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

304. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs 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.

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

306. If Plaintiffs 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.

307. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs 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.

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

309. Plaintiffs and Class Members have no adequate remedy at law.

310. As a direct and proximate result of Defendant's conduct, Plaintiffs 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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) 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.

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

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

COUNT V

Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiffs and the Class)

313. Plaintiffs and the Class re-allege and incorporate all foregoing paragraphs of this Complaint as if fully set forth herein.

314. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

315. Defendant owes a duty of care to Plaintiffs and the Class that requires it to adequately secure Plaintiffs' and Class Members' Private Information.

316. Defendant failed to fulfill their duty of care to safeguard Plaintiffs' and Class Members' Private Information.

317. Plaintiffs and the Class are at risk of harm due to the exposure of their Private Information and Defendant's failure to address the security failings that lead to such exposure.

318. Plaintiffs, therefore, seek a declaration that (1) Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. 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;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. 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;

e. Conducting regular database scanning and security checks;

f. 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;

g. Purchasing credit monitoring services for Plaintiffs and Class Members for a period of ten years; and

h. Meaningfully educating Plaintiffs and Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

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

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

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

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

vi. prohibiting Defendant from maintaining the Private Information of Plaintiffs

and Class Members on a cloud-based database;

vii. requiring Defendant 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 Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant 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 Plaintiffs and Class Members;

xiii. requiring Defendant 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;

xiv. requiring Defendant 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 Defendant's policies, programs, and systems for protecting personal identifying information;

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

xvi. requiring Defendant 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;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xviii. 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 Defendant's 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 damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: March 6, 2024

Respectfully Submitted,

/s/ *Lee A. Floyd*
Lee A. Floyd, VSB #88459
Sarah G. Sauble, VSB #94757
BREIT BINIAZAN, PC
2100 East Cary Street, Suite 310
Richmond, Virginia 23223
Telephone: (804) 351-9040
Lee@bbtrial.com
Sarah@bbtrial.com

Liaison Counsel for Plaintiffs

Terence R. Coates (admitted *Pro Hac Vice*)
Justin C. Walker (admitted *Pro Hac Vice*)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com

Interim Lead Counsel for Plaintiffs

William B. Federman (admitted *Pro Hac Vice*)
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue

Oklahoma City, OK 73120
Telephone: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081
wbf@federmanlaw.com

David K. Lietz (admitted *Pro Hac Vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Courtney L. Weiner (No. 96733)
LAW OFFICE OF COURTNEY WEINER PLLC
1629 K Street, NW, Suite 300
Washington, DC 20006
T: (202) 827-9980
cw@courtneyweinerlaw.com

LAUKAITIS LAW LLC
Kevin Laukaitis (pro hac vice forthcoming)
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Attorneys for Plaintiffs and the Proposed Class