UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

YOCHIA BLEVINS, individually and on behalf of a class of similarly situated individuals, Plaintiffs, v. CONNECTONCALL.COM, LLC and PHREESIA, INC., Defendants.	Case No. **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

1. Plaintiff Yochia Blevins ("Plaintiff" or "Plaintiff Blevins"), individually and on behalf of all other persons similarly situated, and by and through her attorneys, upon personal knowledge as to her own acts and experiences, and upon information and belief as to all other matters alleges as follows:

NATURE OF THE ACTION

2. Plaintiff brings this Class Action Complaint against Defendants ConnectOnCall.com, LLC ("ConnectOnCall") and Phreesia, Inc. ("Phreesia") (collectively, "Defendants") to seek recovery on behalf of herself and 914,138 similarly situated people (the "Class" or "Class Members," defined herein), based upon Defendants' failure to properly secure and safeguard the personally identifiable information ("PII") and personal health information ("PHI") (collectively "Private Information") of individuals receiving Defendants' services.

3. Specifically, upon information and belief, Defendants failed to properly protect Plaintiff's and Class Members' names, phone numbers, and information related to their health

conditions, treatments, or prescriptions. On information and belief, some Class Members' Social Security numbers were also accessed.[1]

4. Defendants provide healthcare related services, including patient-provider communications solutions, to a variety of healthcare organizations and providers located across the country.

5. On May 12, 2024, Defendant Phreesia learned of a service disruption on ConnectOnCall, a product offered by Defendant ConnectOnCall.com, LLC, a subsidiary Phreesia acquired in October 2023.[2] An investigation conducted by Phreesia revealed that between February 16, 2024, and May 12, 2024, an unauthorized actor infiltrated and accessed the inadequately protected computer systems of Defendants (the "Data Breach"). This unauthorized actor was able to access and view the Private Information that was stored on Defendants' computer systems. Defendants did not detect the activity until May 12, 2024, almost three months after the unauthorized actor had breached Defendants' systems.

6. On December 11, 2024, Defendants finally reported the Data Breach to the United States Department of Health and Human Services, Office for Civil Rights, stating that 914,138 individuals have been affected.[3] Defendants waited seven months after it detected the Data Breach to belatedly notify the public of the hacking incident.

---

[1] *ConnectOnCall.com, LLC Provides Notice of Data Security Incident*, Business Wire, https://www.businesswire.com/news/home/20241211221827/en/ConnectOnCall.com-LLC-Provides-Notice-of-Data-Security-Incident (last visited Dec. 24, 2024).

[2] *ConnectOnCall Security Incident Update,* Phreesia, https://www.phreesia.com/security-incident/ (last visited Dec. 24, 2024).

[3] *Cases Currently Under Investigation,* U.S. Department of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Dec. 24, 2024).

7. The large and preventable Data Breach occurred because of Defendants' failure to implement adequate and reasonable cyber-security measures to ensure its computer systems were protected. Because Defendants' data security protocols and practices were deficient, unauthorized actors were able to access, acquire, appropriate, encumber, exfiltrate, steal, use, and/or view Plaintiff's and Class Members' Private Information.

8. Defendants failed to properly safeguard Plaintiff's and Class Members' Private Information. Defendants' negligence has caused over 900,000 Class Members harm and has placed them at a substantially increased risk of identity fraud, which will negatively impact them for years.

9. Despite identifying the breach on May 12, 2024, Defendant did not report the breach until December 11, 2024, seven months after the Data Breach occurred and the sensitive Private Information those individuals affected had been exposed.[4]

10. Defendants' egregious failure to timely detect and report the Data Breach made Plaintiff and Class Members vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Private Information.

11. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach, and assistance in mitigating the effects of the misuse of their Private Information.

12. Defendants and their employees failed to properly monitor the computer network and systems that housed the Private Information. If Defendants had properly maintained and monitored their information technology infrastructure and denied access to that infrastructure to all potential threats, Defendants would have either prevented the Data Breach altogether or, at the very least, limited the extent to which the Private Information was compromised.

[4] *Id.*

13. Defendants had numerous statutory, regulatory, and common law duties to Plaintiff and Class Members to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

14. Defendants disregarded the statutory, regulatory, and common law duties owned to Plaintiff and Class Members by, *inter alia,* intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate and complete notice of the Data Breach.

15. Defendants were and remain required to maintain the security and privacy of the Private Information entrusted to them. When Plaintiff and Class Members provided their Private Information to Defendants, Defendants were required to comply with the obligation to keep Plaintiff's and Class Members' Private Information secure and safe from unauthorized access, to use this information for business purposes only, and to make only authorized disclosures of this information.

16. Defendants were cognizant of the ever-growing and ever-present threat of cybersecurity attacks and the potential for improper disclosure of Plaintiff's and Class Members' Private Information. Despite this awareness, Defendants failed to properly safeguard Plaintiff and Class Members' information. This makes Defendants' failure particularly egregious.

17. By virtue of Defendants' business practices, Defendants represented to Plaintiff and Class Members that their Private Information would be safeguarded.

18. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information by entrusting it to Defendants who represented that it would protect and safeguard their Private Information.

19. Plaintiff and Class Members' Private Information was accessed by one or more unauthorized actors because Defendants failed to properly protect the Private Information of Plaintiff and Class Members.

20. Armed with the Private Information accessed in the Data Breach, cybercriminals now have the means to commit a wide range of crimes, leaving Plaintiff and the Class exposed to ongoing and imminent risk of various forms of identity theft. This threat will persist for the foreseeable future, and Plaintiff and the Class will be forced to remain extra vigilant—constantly monitoring their financial accounts and personal data—due to Defendants' failures, in an attempt to prevent further victimization for the rest of their lives.

21. Defendants' conscious decision to delay notifying Plaintiff and Class Members, for seven months, exacerbated the harm that Plaintiff and Class Members have and will experience. Moreover, as a result of this delay cybercriminals were able to monitor and exploit their unsuspecting victims, leaving them exposed to fraud and further harm—risks they may have been able to mitigate had Defendants disclosed the data breach in a timely manner.

22. As a result of the Data Breach, Plaintiff and Class Members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data

consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) 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 their Private Information.

23. Plaintiff seeks to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed and/or removed from Defendants' network during the Data Breach. Accordingly, Plaintiff brings this class action lawsuit on behalf of herself and a class of individuals whose Private Information was accessed and/or stolen by cybercriminals due to Defendants' negligent and reckless failures to implement reasonable and up-to-date cybersecurity measures to protect Plaintiff's and Class Members' sensitive Private Information.

THE PARTIES

24. Plaintiff Yochia Blevins is, and at times relevant hereto has been, a citizen of the State of Georgia and resides in Liberty County. Plaintiff received a Notice of Data Breach from Defendants, dated December 11, 2024, notifying her that her Private Information had been improperly exposed to unauthorized parties by Defendants between February 16, 2024 and May 12, 2024 (the "Notice Letter").[5]

25. The Notice Letter stated that her Private Information was accessed in the Data Breach:

> **What Happened?** On May 12, 2024, we learned of an issue impacting ConnectOnCall. As soon as we learned of the incident, we immediately began an investigation and took steps to secure the product and ensure the overall security of our environment. Our investigation revealed that between February 16, 2024, and May 12, 2024, an unknown third party had access to ConnectOnCall and certain data within the application, including certain information in provider-patient communications.

[5] Plaintiff Yochia Blevins' Notice Letter is attached hereto as Exhibit A.

> **What Information Was Involved?** You are receiving this notice because you or your family member, health advocate, or healthcare provider provided your information in a patient-provider message using ConnectOnCall. We have determined that the personal information involved in this incident may have included your name, phone number, and information related to your health conditions, treatments, or prescriptions.
>
> **What We Are Doing.** We engaged external cybersecurity specialists to determine the full nature and scope of the incident, identify any impacted information, and help us enhance our security controls to mitigate the risk of future security incidents. Also, after becoming aware of the incident, we took the ConnectOnCall product offline and have been working through a phased restoration of the product in a new, more secure environment. We also notified federal law enforcement of the incident.

26. Defendant Phreesia, Inc., is a citizen of the State of Delaware, with its principal place of business located in Delaware. Defendant Phreesia is a technology and software company that provides solutions to healthcare organizations and providers located across the country, including in New York, for patient check-in and administrative tasks. Phreesia is a publicly traded company with its common stock traded on the New York Stock Exchange under the stock symbol "PHR," and as of December 2024, with a market cap of approximately $1.454 billion.[6]

27. Defendant ConnectOnCall, LLC is a limited liability company organized under the laws of the State of New York, with a principal place of business located at 200 Motor Parkway, Hauppauge, New York. Defendant ConnectOnCall is a software company that specializes in managing and coordinating after-hours phone calls from patients, providers and staff of healthcare organizations and providers. Defendant ConnectOnCall is a wholly owned subsidiary of Defendant Phreesia. Defendant Phreesia acquired Defendant ConnectOnCall on October 3, 2023, for a total consideration of $13.9 million.[7] On information and belief, Phreesia, Inc. is the sole

---

[6] *NYSE – Nasdaq Real Time Price, Phreesia, Inc. (PHR)*, Yahoo Finance, https://finance.yahoo.com/quote/PHR/ (last visited Dec. 24, 2024).

[7] *Phreesia Announces Third Quarter Fiscal 2024 Results,* Phreesia, Dec. 5, 2023 https://ir.phreesia.com/news/news-details/2023/Phreesia-Announces-Third-Quarter-Fiscal-2024-Results/default.aspx (last visited Dec. 24, 2024).

member of ConnectOnCall, LLC, but full and complete LLC membership information, including names, locations, and citizenship of each LLC member, is exclusively in the possession of Defendants ConnectOnCall LLC and Phreesia, Inc.

JURISDICTION AND VENUE

28. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. §1332 of the Class Action Fairness Act of 2005 because this is a class action wherein (a) the amount in controversy exceeds $5,000,000, exclusive of interest and costs; (b) there are more than 100 members of the proposed class; and (c) there is minimal diversity because at least one Plaintiff and one Defendant are citizens of different states. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.

29. This Court has general personal jurisdiction over Defendants pursuant to N.Y. C.P.L.R. § 302 because Defendants Phreesia, Inc. and ConnectOnCall, LLC transact business within the state or contract to supply goods or services in the state, and/or committed a tortious act causing injury to person or property within the state and regularly does or solicits business or derives substantial revenue from services rendered in the state.

30. Venue is proper in this district under 28 U.S.C. §1391(b) because Defendants operate in this district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this district, including Defendants collecting and/or storing the Private Information of Plaintiff and Class Members.

FACTUAL ALLEGATIONS

A. Defendants Acquire, Collect, and Maintain Plaintiff's and Class Members' Private Information

31. Defendants offer software solutions to healthcare organizations and providers. These software solutions are focused on streamlining and supporting the administrative aspects of

healthcare, including patient intake and communications. In providing its services, Defendants require Plaintiff and Class Members to provide their highly sensitive Private Information.

32. At times relevant to this action, Defendant ConnectOnCall offered a product entitled ConnectOnCall, which assists providers and patients in after-hours communications. After Defendant Phreesia's acquisition of ConnectOnCall in October 2023, Defendants began offering ConnectOnCall's after-hours communications product to its customers under the name "PhreesiaOnCall."[8] For the purposes of this action, plaintiffs may sometimes refer to the products as the "OnCall Product."

33. When patients, including Plaintiff and Class Members, utilize the OnCall Product to communicate with their providers, any relevant information available in other integrated systems are matched with the patient-caller using "Phreesia's bidirectional EHR [Electronic Health Record] integration… allowing the provider to review a snapshot of the patient's history before returning the call."[9]

34. Defendant Phreesia also offers services that assist with the patient check-in process[10] and health screening questionnaires,[11] among others. These services require that Plaintiff and Class Members enter their Private Information into a digital check-in form[12] or questionnaire[13] to receive medical and/or health related services. Upon information and belief, Private Information

[8] *After Hours*, Phreesia, https://www.phreesia.com/after-hours/ (last visited Dec. 24, 2024).
[9] *Id.*
[10] *Registration,* Phreesia, https://www.phreesia.com/products/registration/ (last visited Dec. 24, 2024).
[11] *Collect Patient-Reported Data,* Phreesia, https://www.phreesia.com/products/collect-patient-reported-data/ (last visited Dec. 24, 2024).
[12] *Registration, supra,* note 10.
[13] *Collect Patient-Reported Data, supra* note 11.

provided to Phreesia through their other services may populate within the "snapshot" shown to providers.

35. Defendants failed to protect Plaintiff's and Class Members' Private Information because an unauthorized actor accessed Plaintiff and Class Members' Private Information during the Data Breach without their consent.

36. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure. In other words, by collecting and storing this Private Information, Defendants assumed an obligation to protect it.

37. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Defendants were required to keep Plaintiff's and Class Members' Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

B. The Data Breach and Defendants' Failure to Timely Disclose the Same

38. On May 12, 2024, Defendants learned of a service disruption to "ConnectOnCall."[14] After an investigation Defendants discovered that beginning on February 16, 2024, and continuing through May 12, 2024, an unknown third party had gained access to Defendants' computer systems.[15] During that period, Private Information that was stored on Defendants' systems was accessed and viewed by the unauthorized actor(s).[16]

[14] *See ConnectOnCall Security Incident Update, supra* note 2.
[15] *Id.*
[16] *Id.*

39. Defendants reported to the United States Department of Health and Human Services, Office for Civil Rights, that the Data Breach affected 914,138 individuals.[17]

40. Despite knowing of the Data Breach incident as early as May 12, 2024, and despite obligations to provide adequate and timely notice so that affected persons can take precautions and mitigate potential losses and damages, Defendants did not begin to file notices with state attorney general offices or notify individuals of the Data Breach until December 11, 2024.

41. In its Notice Letter, Defendants failed to provide basic details such as how the unauthorized actor(s) accessed their networks, whether the data accessed was encrypted or otherwise protected, and how it learned of the Data Breach.[18]

42. The Data Breach occurred because Defendants did not implement adequate and reasonable cyber-security procedures and protocols to protect the Private Information of Plaintiff and Class Members. Because Defendants' data security protocols and practices were deficient, unauthorized person(s) were able to access, view, and/or exfiltrate Plaintiff's and Class Members' Private Information.

43. In the Notice Letter, Defendants acknowledged that upon discovery of the Data Breach, they "engaged external cybersecurity specialists to… help [them] enhance [their] security controls to mitigate the risk of future security incidents" and that the product was taken offline until it can be restored in a "new, more secure environment."[19] The fact that Defendants enhanced its security features after learning of the Data Breach demonstrates that their cybersecurity measures were inadequate, negligent, and otherwise lacking at the time of the Data Breach.

[17] *See Cases Currently Under Investigation, supra* note 3.
[18] *See* Plaintiff Blevins' Notice Letter attached hereto as Exhibit A.
[19] *Id.*

44. Furthermore, Defendants' Notice Letter disclosed that the types of information compromised by the Data Breach generally included individuals' names, phone number, and information related to their health conditions, treatments, or prescriptions. On information and belief, some Class Members' Social Security numbers were also accessed.[20]

45. Given the intentional and criminal nature of the cybersecurity hack, the data accessed in the Data Breach was likely exfiltrated and sold and/or publicly posted on the internet.

46. The Notice Letter sent to Plaintiff, and upon information and belief to other Class Members, failed to offer any identity theft protection services whatsoever. This is wholly inadequate because data breach victims and victims of other unauthorized disclosures commonly face numerous years of ongoing identity theft. Indeed, Defendants informed Class Members to "remain vigilant by reviewing account statements and monitoring free credit reports," and to even take the step of "temporarily freez[ing] your credit."[21]

47. The Notice Letter also suggested several additional time-consuming steps that Plaintiff and Class Members could take to protect themselves as a result of the Data Breach, including obtaining credit reports from credit reporting agencies, freezing their credit, placing fraud alerts, and/or contacting government authorities.

48. Given Defendants' recommendation that Plaintiff and Class Members take these mitigating actions, along with its decision to offer credit monitoring services to the affected individuals, it is evident that the risks stemming from the Data Breach are both real and substantial.

C. Plaintiff's Experience

[20] *ConnectOnCall.com, LLC Provides Notice of Data Security Incident, supra* note 1.
[21] *See* Plaintiff Blevins' Notice Letter attached hereto as Exhibit A..

49. Plaintiff entrusted her Private Information to Defendants in order to receive Defendants' services.

50. Plaintiff received a letter from Defendants, dated December 11, 2024, informing her that her name, phone number, and information related to her health conditions, treatments, or prescriptions had been disclosed to an unknown actor as a result of the Data Breach.[22]

51. Plaintiff has taken steps to secure her Private Information and implemented a freeze on her credit with national credit reporting agencies.

52. Because the Data Breach was an intentional attack by cybercriminals seeking valuable information that they could exploit, Plaintiff remains at critical risk of severe identity theft and exploitation.

53. Plaintiff is very careful about not sharing her sensitive Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

54. Plaintiff takes great care to store any documents containing her personal information in secure locations or to properly dispose of such documents. She also exercises caution by selecting unique usernames and strong passwords for her online accounts to protect her privacy and security.

55. Plaintiff has suffered imminent and ongoing harm due to the significantly heightened risk of fraud, identity theft, and misuse resulting from the unauthorized exposure of her Private Information to third parties, including potentially criminal actors.

[22] *Id.*

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

D. Defendants Had Obligations to Protect Personal Information Under Federal and State Law and the Applicable Standards of Care

57. Defendants maintain and store the Private Information of Plaintiff and the Class in the usual course of business.

58. In collecting, maintaining, and storing Private Information, Defendants promise to keep such information confidential and protect it from third parties.

59. In its Privacy Policy, Defendants represent that "[p]rivacy and security are top priorities to [them]-not boxes to be checked during a once-a-year review."[23] The Privacy Policy further states that "at every level of [their] organization, [they] have measures and protocols in place to protect your information, and [they] foster a culture focused on safeguarding data.[24]

60. Defendants further claim that they "believe everyone should be in charge of their health information," and that they've "built [their] platform of personalized health content on the principles of privacy and consent."[25]

61. Under the Federal Trade Commission Act ("FTCA") (15 U.S.C. § 45), Defendants were prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has determined that a company's failure to implement reasonable and appropriate data security measures to protect consumers' sensitive personal

[23] *Privacy Policy,* Phreesia, https://www.phreesia.com/privacy-policy/ (last visited Dec. 24, 2024).
[24] *Id.*
[25] *Our Commitment to Privacy,* Phreesia, https://www.phreesia.com/our-commitment-to-privacy/ (last visited Dec. 24, 2024).

information constitutes an "unfair practice" in violation of the Act. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

62. Defendants are also required by various state laws and regulations to protect Plaintiff's and Class Members' Private Information.

63. In addition to their obligations under federal and state laws, Defendants had a duty to Plaintiff and Class Members whose Private Information was entrusted to its care. This duty required Defendants to exercise reasonable care in acquiring, retaining, securing, safeguarding, deleting, and protecting that information from compromise, loss, theft, unauthorized access, or misuse. Defendants owed Plaintiff and the Class Members an obligation to provide reasonable security measures, in line with industry standards and regulatory requirements, ensuring that its computer systems, networks, and personnel responsible for them adequately protected the Private Information of Plaintiff and the Class Members from unauthorized exposure.

64. Defendants owed a duty to Plaintiff and the Class Members, whose Private Information was entrusted to Defendants' care, to design, maintain, and regularly test its computer and email systems to ensure that the Private Information in its possession was adequately secured and protected from unauthorized access or compromise.

65. Defendants owed a duty to Plaintiff and the Class Members, whose Private Information was entrusted to its care, to establish and enforce reasonable data security practices and procedures to protect that information. This duty included properly training its employees and others with access to Private Information within its computer systems on how to securely handle and protect such data.

66. Defendants owed a duty to Plaintiff and the Class Members, whose Private Information was entrusted to Defendants' care, to maintain, update and otherwise ensure the security of the OnCall Product upon the acquisition of ConnectOnCall.

67. Defendants owed a duty to Plaintiff and the Class Members, whose Private Information was entrusted to its care, to implement processes capable of detecting, investigating and thwarting a breach in its data security systems in a timely manner.

68. Defendants owed a duty to Plaintiff and the Class Members, whose Private Information was entrusted to its care, to disclose if its computer systems and data security practices were inadequate to protect individuals' Private Information from theft. Such an inadequacy would constitute a material fact in the decision to entrust personal information to Defendant.

69. Defendants owed a duty to Plaintiff and the Class Members, whose Private Information was entrusted to its care, to promptly and accurately disclose any data breaches that occurred.

70. Defendants owed a duty of care to Plaintiff and the Class Members, as they were foreseeable and likely victims of any deficiencies in Defendants' data security practices.

E. Defendants Could Have and Should Have Prevented This Data Breach

71. Despite the growing body of publicly available information regarding the rise of ransomware attacks and other forms of cyberattacks that compromise Private Information, Defendants' approach to maintaining the privacy of Plaintiff and Class Members' Private Information was inadequate, unreasonable, negligent, and reckless. This is evidenced by Defendants' acknowledgment that additional steps have been taken post-Data Breach to enhance its existing security measures. Defendants' Notice Letter admits that at the time of the Data Breach

its technical and cybersecurity capabilities were inadequate, which in turn caused the Data Breach and the divulgence of Plaintiff and Class Members' Private Information.

72. The Data Breach was clearly foreseeable to Defendants. It is well known, and is further alleged below, that cyber-attacks against critical infrastructure companies such as Defendants are targeted and frequent. Such data breaches against the critical infrastructure have become widespread.

73. The Cybersecurity and Infrastructure Security Agency ("CISA") of the United States has the healthcare and health sector as critical infrastructure.[26] As a provider of critical infrastructure, Defendants knew or should have known that there was a significant risk of a cyber-attack on its computer networks and systems. The Department of Homeland Security states that "[c]ybersecurity threats to critical infrastructure are one of the most significant strategic risks for the United States."[27]

74. The Data Breach was also clearly foreseeable to Defendants as they are business associates of the healthcare and health sector. Cyber-attacks on business associates have skyrocketed in recent years. In 2023, more than 93 million healthcare records were exposed or stolen in data breaches targeted towards business associates compared to 34.9 million in breaches targeted towards healthcare providers.[28]

---

[26] *Critical Infrastructure Sectors*, Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (lasted visited Dec. 24, 2024).
[27] *Secure Cyberspace and Critical Infrastructure*, Department of Homeland Security (DHS), https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure (last visited Dec. 24, 2024).
[28] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Dec. 24, 2024).

75. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendants could and should have implemented the following preventive measures, as recommended by the United States Government:

- **Implement an awareness and training program:** Educate employees and individuals about the threat of ransomware and how it is delivered, as end users are often the primary targets.

- **Enable strong spam filters:** Prevent phishing emails from reaching end users by using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to block email spoofing.

- **Scan all incoming and outgoing emails:** Detect threats by scanning emails and filtering executable files to prevent them from reaching end users.

- **Configure firewalls:** Block access to known malicious IP addresses to prevent unauthorized access.

- **Patch operating systems, software, and firmware:** Regularly update and patch devices, potentially using a centralized patch management system for greater efficiency.

- **Set anti-virus and anti-malware programs for regular scans:** Ensure these programs run automatic scans to detect and remove potential threats.

- **Manage privileged accounts based on the principle of least privilege:** Limit administrative access to users only when absolutely necessary, and ensure those with admin privileges use them only when required. Implement an awareness and training program.

- **Configure access controls:** Implement least privilege principles for file, directory, and network share permissions. Users should only have access to what they need—if a user only needs to read specific files, they should not have write access to those files, directories, or shares.

- **Disable macro scripts in office files transmitted via email:** Prevent the execution of potentially harmful macros by disabling them in office files sent via email. Consider using Office Viewer software instead of full office suite applications to open email attachments.

- **Implement Software Restriction Policies (SRP):** Use SRPs or similar controls to prevent programs from executing from common ransomware locations, such as

temporary folders associated with web browsers or compression programs, including the AppData/LocalAppData folder.

- **Disable Remote Desktop Protocol (RDP):** If RDP is not in use, consider disabling it to reduce potential attack vectors.

- **Use application whitelisting:** Allow only programs that are explicitly permitted by security policy to execute, blocking any unauthorized or potentially malicious software.

- **Execute operating system environments or specific programs in a virtualized environment:** Run sensitive systems or programs in isolated virtual environments to reduce risk.

- **Categorize data based on organizational value:** Implement physical and logical separation of networks and data for different organizational units to protect critical information and ensure appropriate access control.[29]

76. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendants could and should have implemented the following preventive measures, as recommended by Microsoft's 2023 Digital Defense Report:

- **Enable multifactor authentication (MFA)**. This protects against compromised user passwords and helps to provide extra resilience for identifies.

- **Apply Zero Trust principles.** This includes ensuring users and devices are in a good state before allowing access to resources, allowing only the privilege that is needed for access to a resource and no more, assuming system defenses have been breached and systems may be compromised.

- **Use extended detection and response (XDR) and antimalware**. Implement software to detect and automatically block attacks and provide insights into the security operations software.

- **Keep up to date**. Unpatched out-of-date systems are a key reason many organizations fall victim to cyber-attacks.

---

[29] *How to Protect Your Networks from Ransomware: Technical Guidance Document,* United States Department of Justice, https://www.justice.gov/criminal/criminal-ccips/file/872771/dl#:~:text=The%20U.S.%20Government%20(USG)%20recommends,and%20Conformance%20(DMARC)%2C%20and (last visited Dec. 24, 2024).

- **Protect data**. Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.[30]

77. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendants could and should have implemented the following preventive measures, as recommended by the FTC in its latest update to *Protecting Personal Information: A Guide for Business*:

- Know what personal information you have in your files and on your computers.
- Keep only what you need for your business.
- Protect the information that you keep.
- Properly dispose of information you no longer need.
- Create a plan to respond to security incidents.[31]

78. To mitigate the heightened risk of ransomware attacks and other data breaches, including the incident that led to the Data Breach, Defendants could and should have implemented the following preventive measures, as recommended by the Joint Ransomware Task Force's ("JRTF") #StopRansomware Guide, although this list does not encompass the full range of recommended actions:

- **Conduct regular vulnerability scanning to identify and address vulnerabilities**, especially those on internet-facing devices, to limit the attack surface.
- **Regularly patch and update software and operating systems to the latest available versions.** Prioritize timely patching of internet-facing servers-that operate software for processing internet data such as web browsers, browser plugins, and document readers-especially for known exploited vulnerabilities….

---

[30] *Microsoft Digital Defense Report 2023*, Microsoft https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023 (last visited Dec. 24, 2024)
[31] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Dec. 24, 2024).

- **Limit the use of RDP and other remote desktop services.** If RDP is necessary, apply best practices. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later traverse the network using the native Windows RDP client.

- **Ensure all on-premises, cloud services, mobile, and personal devices are properly configured, and security features are enabled**. For example, disable ports and protocols that are not being used for business purposes.[32]

79. Given that Plaintiff and the Class Members provided Private Information to Defendants, Defendants should have and could have taken the above measures to ensure that the Private Information entrusted to its care was safe from unauthorized actors.

80. The occurrence of the Data Breach indicates that Defendants failed to implement one or more of the above measures to prevent ransomware attacks. The failure to implement some or all of the above measures resulted in the Data Breach and the exposure of over two hundred thousand Class Members' Private Information.

F. Defendants Failed to Comply with FTC Guidelines

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

82. For example, in 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines advise businesses, inter alia, to protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information

[32] *#StopRansomware Guide*, Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/resources-tools/resources/stopransomware-guide (last visited Dec. 24, 2024).

stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[33]

83. The guidelines further advise businesses: not to maintain PII longer than necessary for authorization of a transaction; to limit access to sensitive data; to use an intrusion detection system to expose a breach as soon as it occurs; to 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 to verify that third-party service providers have implemented reasonable security measures.[34]

84. To underscore the binding significance and legal ramifications of the promulgated guidance, 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 FTCA, 15 U.S.C. § 45.[35] Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

85. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duties in this regard.

---

[33] *Protecting Personal Information: A Guide for Business,* Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Dec. 24, 2024).

[34] *Id.*

[35] *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015) (determining that a company's failure to implement reasonable and appropriate data security measures to protect consumers' sensitive personal information constitutes an "unfair practice" in violation of the Act).

86. Defendants failed to properly implement basic data security practices.

87. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information, or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

88. Upon information and belief, Defendants were at all times fully aware of their obligations to protect the Private Information of Plaintiff and Class Members, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendants' 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 Plaintiff and the Class.

G. Defendants Failed to Comply with HIPAA Guidelines

89. Defendants are covered entities under Health Insurance Portability and Accountability Act ("HIPAA") (45 C.F.R. § 160.102) and as such were required to protect against reasonably anticipated threats to the security of Private Information in its systems. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[36]

90. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for

[36] *What is Considered Protected Health Information Under HIPAA?*, The HIPAA Journal, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last visited Dec. 24, 2024).

handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

91. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendants to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[37]

92. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations. Defendants' security failures include, but are not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendants create, receive, maintain, and transmit in violation of 45 C.F.R. §164.306(a)(1);

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

c. 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);

d. Failing to identify and respond to suspected or known security incidents; 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);

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

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually

[37] *Breach Notification Rule*, U.S Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Dec. 24, 2024).

identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. §164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

i. Failing to effectively train all members of its workforce (including agents and independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

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

93. At all times, Defendant was fully aware of its responsibilities under HIPAA to safeguard consumers' private information, as reflected in its own privacy statement, yet it failed to meet these obligations. The Defendant also understood the serious consequences that would arise from its failure to comply. Given the nature and volume of the private information it collected and stored, as well as the foreseeable damages that could result, Defendant's actions were particularly egregious.

H. Plaintiff and Class Members Suffered Damages

94. The ramifications of Defendants' failure to safeguard the Private Information of Plaintiff and Class Members are long-lasting and severe. In 2023 alone, American adults lost $43

billion to identity theft.[38] Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

95. As a result of the Data Breach, Plaintiff's and Class Members' Private Information has diminished in value.

96. The Private Information belonging to Plaintiff and Class Members is private in nature and was left inadequately protected by Defendants who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standard.

97. The Data Breach was a direct and proximate result of Defendants' failure to: (a) properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

98. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately implement proper data security measures, despite its obligation to protect the Private Information.

---

[38] *Identity Fraud Cost Americans $43 Billion in 2023*, AARP, https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html#:~:text=Victims%20are%20losing%20more%20money,new%20AARP%2Dbacked%20report%20finds&text=American%20adults%20lost%20a%20total,new%20report%20cosponsored%20by%20AARP. (last visited Dec. 24, 2024).

99. Had Defendants remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

100. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

101. Defendants' failure to adequately protect Plaintiff's and Class Members' Private Information has resulted in Plaintiff and the Class Members having to undertake these tasks which require extensive amounts of time, calls and, for many of the credit and fraud protection services. As Defendants' Notice Letter indicates, Defendants are putting the burden on Plaintiff and the Class Members to discover possible fraudulent activity and identity theft.

102. As a result of Defendants' failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at an increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Unauthorized use and misuse of their Private Information;

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

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual

and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

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

g. The continued risk to their Private Information that is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the Private Information in their possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

103. In addition to a remedy for economic harm, Plaintiff and the Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

CLASS ALLEGATIONS

104. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiff seeks to bring this class action on behalf of herself and a class (the "Class") defined as follows:

> **All persons whose Private Information was accessed and/or acquired in the ConnectOnCall.com, LLC data incident that occurred in or around February through May 2023.**

105. Excluded from the Class are Defendants and their officers; directors and employees; any entity in which Defendants have a controlling interest, is a parent or subsidiary, or

which is controlled by Defendants; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendants. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

106. Plaintiff reserves the right to modify and/or amend the Class, including, but not limited to, creating additional subclasses as necessary.

107. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

108. ***Numerosity.*** Consistent with Fed. R. Civ. P. 23(a)(l), the Class is so numerous that joinder of all members is impracticable. Defendants have acknowledged that the number of members of the Class exceeds 900,000. All Class Members are readily ascertainable in that Defendants have access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

109. ***Commonality and Predominance.*** Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), this action involves common questions of law and fact that predominate over any questions that may affect only individual Class Members. Such common questions include:

a. Whether Defendants failed to adequately safeguard Plaintiff's and the Classes' Private Information;

b. Whether Defendants failed to protect Plaintiff's and the Class Members' Private Information;

c. Whether Defendants' computer systems and data security practices used to protect Plaintiff's and the Class Members' Private Information violated the FTCA, state laws, and/or Defendants' other duties;

d. Whether Defendants violated the data security statutes and data breach notification statutes applicable to Plaintiff and the Class;

e. Whether Defendants failed to notify Plaintiff and Class Members about the Data Breach expeditiously and without unreasonable delay after the Data Breach was discovered;

f. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information properly as promised;

g. Whether Defendants acted negligently in failing to safeguard Plaintiff's and the Class Members' Private Information;

h. Whether Defendants violated the consumer protection statutes, data breach notification statutes, and state privacy statues applicable to Plaintiff and the Class;

i. Whether Defendants failed to notify Plaintiff and Class Members about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

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

k. What equitable relief is appropriate to redress Defendants' wrongful conduct; and

l. What injunctive relief is appropriate to redress the imminent and current ongoing harm faced by Plaintiff and the Class Members.

110. ***Typicality***: Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of the claims of other Class Members in that Plaintiff, like all Class Members, had her personal data compromised, breached, and stolen in the Data Breach. Plaintiff and all Class Members were injured through the misconduct of Defendants and assert the same claims for relief.

111. ***Adequacy***: Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Plaintiff is a member of the Class she seeks to represent; is committed to pursuing this matter against Defendants to obtain relief for the Class; and has no interests that are antagonistic to, or in conflict with, the interests of other Class Members. Plaintiff retained counsel who are competent and experienced in litigating class actions and complex litigation, including data breach litigation of this kind. Plaintiff and her counsel intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

112. ***Superiority***: Consistent with Fed. R. Civ. P. 23(6)(3), 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. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

113. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3) because the common questions of law or fact predominate over any questions affecting Plaintiff or any individual Class Members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

114. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(l) because the prosecution of separate actions by the 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 Defendants. By contrast, conducting this litigation as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendants to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

115. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants, through their uniform conduct, acted or failed and refused to act on grounds generally applicable to Plaintiff and the Class as a whole, making injunctive and declaratory relief appropriate to Plaintiff and the Class as a whole. Moreover, Defendants continue to maintain their inadequate security practices, retain possession of Plaintiff's and Class Members' Private Information, and have not been forced to change their practices or to relinquish Private Information by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

116. Particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present discrete common issues, the resolution of which would materially

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

a. whether Plaintiff's and Class Members' Private Information was accessed, compromised, or stolen in the Data Breach;

b. whether Defendants owed a legal duty to Plaintiff and Class Members;

c. whether Defendants failed to take adequate and reasonable steps to safeguard the Private Information of Plaintiff and Class Members;

d. whether Defendants failed to adequately monitor its data security systems;

e. whether Defendants failed to comply with applicable laws, regulations, and industry standards relating to data security;

f. whether Defendants knew or should have known that it did not employ adequate and reasonable measures to keep Plaintiff's and Class Members' Private Information secure; and

g. whether Defendants' adherence to FTC data security obligations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

COUNT ONE
Negligence
(On Behalf of Plaintiff and the Class)

117. Plaintiff repeats and re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 116.

118. Plaintiff brings this claim on behalf of herself and the Class.

119. Defendants gathered and stored the Private Information of Plaintiff and Class Members as part of the regular course of its business operations. Plaintiff and Class Members

were entirely dependent on Defendants to use reasonable measures to safeguard their Private Information and were vulnerable to the foreseeable harm described herein should Defendants fail to safeguard their Private Information.

120. Plaintiff and Class Members entrusted Defendants with their Private Information and Defendants was fully cognizant of the value and importance of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

121. Defendants negligently created a dangerous situation by failing to take adequate and reasonable steps to safeguard Plaintiff's and Class Members' sensitive Private Information from unauthorized release or theft.

122. Defendants owed an independent duty to Plaintiff and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive Private Information, and preventing the Private Information from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

123. Defendants were required to prevent foreseeable harm to Plaintiff and Class Members.

124. Accordingly, Defendants had a duty to take adequate and reasonable steps to safeguard their sensitive Private Information from unauthorized release or theft. Defendants' duties included, but were not limited to: (a) designing, maintaining, and testing its data security systems, data storage architecture, and data security protocols to ensure Plaintiff's and Class Members' Private Information in its possession was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of its security systems and data storage architecture in a timely and adequate manner; (c) timely acting on all warnings and alerts, including

public information, regarding its security vulnerabilities and potential compromise of the Private Information of Plaintiff and Class Members; and (d) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements, including, *inter alia*, Section Five of the FTCA. *See* 15 U.S.C. § 45.

125. Defendants owed a common law duty to prevent foreseeable harm to Plaintiff and Class Members. The duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices of Defendants in their collection, storage, and use of Private Information from Plaintiff and Class Members. It was foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their Private Information because malicious actors routinely attempt to steal such information for nefarious purposes.

126. Additionally, the policy of preventing future harm weighs in favor of finding Defendants owed duties towards Plaintiff and Class Members.

127. Defendants also owed a duty to timely disclose the material fact that its computer systems and data security practices and protocols were inadequate to safeguard Plaintiff's and Class Members' personal, health, and financial data from theft.

128. The injuries suffered by Plaintiff and Class Members were proximately and directly caused by Defendants' failure to follow reasonable, industry standard security measures to protect Plaintiff's and Class Members' Private Information.

129. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take additional steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

130. If Defendants had implemented the requisite industry-standard security measures and exercised adequate and reasonable care, data thieves would not have been able to take the Private Information of Plaintiff and Class Members.

131. Defendants breached these duties through the conduct alleged here in this Complaint by, including without limitation, failing to protect the Private Information in its possession; failing to maintain adequate computer systems and allowing unauthorized access to and exfiltration of Plaintiff's and Class Members' Private Information; failing to disclose the material fact that Defendants' computer systems and data security practices were inadequate to safeguard the Private Information in its possession from theft; and failing to disclose in a timely and accurate manner to Plaintiff and Class Members the material fact of the Data Breach.

132. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, their Private Information would not have been compromised. And, as a direct and proximate result of Defendants' failure to exercise adequate and reasonable care and use commercially adequate and reasonable security measures, the Private Information of Plaintiff and Class Members was accessed by ill-intentioned individuals who could use the information to commit identity or financial fraud. Plaintiff and Class Members face the imminent, certainly impending, and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

133. There is a temporal and close causal connection between Defendants' failure to implement security measures to protect the Private Information collected from Class Members and the harm suffered, or risk of imminent harm suffered, by Plaintiff and Class Members.

134. It was foreseeable that Defendants' failure to exercise reasonable care to safeguard the Private Information in its possession or control would lead to one or more types of injury to

Plaintiff and Class Members. The Data Breach was also foreseeable given the increasing occurrence of cyberattacks and data breaches.

135. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of or should have known of the inherent risks in collecting and storing Private Information, the critical importance of providing adequate security of Private Information, the current cyber hacks being perpetrated on Private Information, and that it had inadequate protocols, including security protocols in place to secure the Private Information of Plaintiff and Class Members.

136. Defendants' own conduct created the foreseeable risk of harm to Plaintiff and Class Members. Defendants' misconduct includes their failure to take the steps and opportunities to prevent the Data Breach and their failure to comply with industry standards for the safekeeping and encrypted authorized disclosure of the Private Information of Plaintiff and Class Members.

137. Plaintiff and Class Members have no ability to protect their Private Information that was and is in Defendants' possession. Defendants alone were, and are, in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

138. As a direct and proximate result of Defendants' negligence as alleged above, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Unauthorized use and misuse of their Private Information;

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

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

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

g. The continued risk to their Private Information that is subject to further breaches so long as Defendants fails to undertake appropriate measures to protect the Private Information in Defendants' possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

COUNT TWO
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

139. Plaintiff repeats and re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 116.

140. Plaintiff brings this claim on behalf of herself and the Class.

141. Pursuant to the FTCA (15 U.S.C. §45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

142. The FTCA prohibits "unfair ... practices in or affecting commerce," which includes, as interpreted and enforced by the FTC, the unfair practice of failing to implement reasonable measures to protect Private Information. The FTC publications and orders mentioned above also contributed to the basis of Defendants' duty in this regard.

143. Pursuant to HIPAA, Defendants had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

144. Defendants solicited, collected, and stored Private Information of Plaintiff and Class Members to facilitate transactions that affect commerce.

145. Defendants breached their duties to Plaintiff and Class Members under the FTCA (15 U.S.C. §45) and HIPAA (42 U.S.C. §§1302d, *et seq*.), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

146. Defendants' failure to comply with relevant laws and regulations constitutes negligence *per se*.

147. Plaintiff and the Class are within the class of persons the FTCA and HIPAA were intended to protect.

148. The harm caused by the Data Breach is the type of harm that the FTCA, HIPAA, and state data breach privacy statutes were designed to prevent.

149. Defendants breached their duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

150. Defendants breached their duties to Plaintiff and the Class by negligently and unreasonably delaying the provision of notice regarding the Data Breach, failing to provide such notice expeditiously or as soon as practicable.

151. Defendants' violation of the FTCA, HIPAA, state data security statutes, and/or state data breach notification statutes constitute negligence per se.

152. As direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach by, *inter alia,* having to spend time reviewing their accounts and credit reports for unauthorized activity; spend time and incur costs to place a re-new "freeze" on their credit; be inconvenienced by the credit freeze, which requires them to spend extra time unfreezing their account with each credit bureau any time they want to make use of their own credit; and becoming a victim of identity theft, which may cause damage to their credit and ability to obtain insurance, medical care, and jobs.

153. The injury and harm that plaintiff and class members suffered (all alleged above) was the direct and proximate result of Defendants' negligence *per se*.

COUNT THREE
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

154. Plaintiff repeats and re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 116.

155. Plaintiff brings this claim on behalf of herself and the Class.

156. A relationship existed between Plaintiff, Class Members and Defendants in which Plaintiff and the Class entrusted Defendants with their Private Information, relying on Defendants' own privacy statements that "at every level of [their] organization, [they] have measures and

protocols in place to protect your information, and [they] foster a culture focused on safeguarding data."

157. By accepting and retaining Plaintiff and the Class Members' Private Information, there was an understanding between the parties that Defendants would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of the Private Information.

158. Plaintiff and the Class Members entrusted their Private Information to Defendants on the premise, and with the understanding, that Defendants would safeguard their information, use their Private Information for business purposes only, and refrain from disclosing, or allowing to be disclosed, their Private Information to unauthorized third-parties.

159. Defendants knew or should have known that the failure to exercise due care in the collecting, storing, and using of individuals Private Information involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third-party.

160. Defendants' fiduciary duty required them to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing its security protocols to ensure that Plaintiff's and the Class Members' Private Information in Defendants' possession was adequately secured and protected.

161. Defendants also had a fiduciary duty to have procedures in place to detect and prevent improper access and misuse of Plaintiff's and the Class Members' Private Information. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and the Class. That special relationship arose because Defendants were entrusted with Plaintiff and the Class Members' Private Information.

162. Defendants breached their fiduciary duty that they owed to Plaintiff and the Class by failing to act in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and by failing to protect the Private Information of Plaintiff and the Class Members.

163. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class Members have suffered and/or will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Private Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (d) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of Defendants' services they received.

164. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and the Class Members have suffered, and will continue to suffer, from other forms of injury and/or harm, both economic and non-economic.

COUNT FOUR
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

165. Plaintiff repeats and re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 116.

166. Plaintiff brings this claim on behalf of herself and the Class.

167. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

168. Defendants owed a duty to Plaintiff and Class Members to keep their Private Information confidential.

169. Defendants affirmatively and recklessly disclosed Plaintiff and Class Members' Private Information to unauthorized third parties.

170. The unauthorized disclosure and/or acquisition by a third party of Plaintiff and Class Members' Private Information is highly offensive to a reasonable person.

171. Defendants' reckless and negligent failure to protect Plaintiff and Class Members' Private Information constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

172. In failing to protect Plaintiff's and Class Members' Private Information, Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

173. Because Defendants failed to properly safeguard Plaintiff's and Class Members' Private Information, Defendants had notice of and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

174. Defendants knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

175. As a proximate result of Defendants' acts and omissions, Plaintiff's and the Class Members' private and sensitive Private Information was stolen by a third party and is now likely available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

176. Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information is still maintained by Defendants with their inadequate cybersecurity system and policies.

177. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard Plaintiff's and the Class Members' Private Information.

178. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT FIVE
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

179. Plaintiff repeats and re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 116.

180. Plaintiff brings this claim on behalf of herself and the Class.

181. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

182. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard their customers' Private Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information.

183. Plaintiff(s) allege that Defendants' data security measures remain inadequate. Plaintiff and Class Members will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

184. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, and Section 5 of the FTCA;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

185. The Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and the Class Members' Private Information.

186. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

187. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach of Defendants' data occurs, Plaintiff and Class Members will be even more likely to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

188. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach by Defendants, thus eliminating the additional injuries that would result to Plaintiff and all consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendants as follows:

a. That the Court certify this case as a class action and certify the Class as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

b. That Plaintiff and the Class be granted the declaratory and injunctive relief sought herein;

c. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as it just and proper in an amount to be determined at trial;

d. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

e. That the Court award pre- and post-judgment interest at the maximum legal rate; and

f. That the Court grant all such other relief as it deems just and proper

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any

and all issues in this action so triable as of right.

Dated: December 24, 2024

Respectfully submitted,

/s/ Lori G. Feldman
GEORGE FELDMAN MCDONALD, PLLC
Lori G. Feldman, Esq.
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Telephone: (917) 983-9321
lfeldman@4-justice.com
eservice@4-justice.com

Attorney for Plaintiff and the Proposed Class

Public court record.

This copy was downloaded from https://storage.courtlistener.com/recap/gov.uscourts.nyed.525473/go
on 2026-10-19 and is hosted, unaltered, for reference at
https://chimo.ai/class-action/connectoncall

Court: U.S. District Court for the Eastern District of New York
Case number: 2:24-cv-08790-SJB-JMW
Filed: 2024-12-24

Chimo hosts public court records for readers' reference; documents are
unaltered copies from the court docket or the court-approved settlement website.