IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

JENNI BARRETTE, on behalf of herself and all others similarly situated, **Plaintiff** **v.** FREEDMAN HEALTHCARE, LLC **Defendant**	Case No.: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Jenni Barrette ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Freedman Healthcare, LLC ("Defendant" or "Freedman Healthcare"). Plaintiff seeks to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Freedman Healthcare allege upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and data breach on Freedman Healthcare's network that resulted in unauthorized access to highly sensitive patient data. Plaintiff brings this class action against Defendant for its failure to secure and safeguard the data of over 40,000 people. As a result, Plaintiff and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their

time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their sensitive Private Information.

2. Defendant Freedman Healthcare is a Massachusetts based software company that offers a range of software products and services to corporate and governmental entities throughout the United States.

3. Freedman Healthcare received PII from state governments. These states possessed and controlled Plaintiff's PII in order for Plaintiff to access health and public assistance programs, as well as government benefits.

4. During its business operations, Defendant acquired, collected, utilized, and derived a benefit from Plaintiff's and Class members' PII. Therefore, Defendant owed and otherwise assumed statutory, regulatory, contractual, and common law duties and obligations, including to keep Plaintiff's and Class members' PII confidential, safe, secure, and protected from the type of unauthorized access, disclosure, and theft that occurred in the Data Breach described below.

5. Despite its duties to Plaintiff and Class members, Freedman Healthcare stored, maintained, and/or hosted Plaintiff's and Class members' PII on its servers negligently and/or recklessly configured and maintained so as to contain security vulnerabilities that resulted in a breach of its network and systems. As a result of the breach, unauthorized third-party cybercriminals gained access to and obtained Plaintiff's and Class members' PII.

6. On or about May of 2025, Freedman Healthcare provided notice that hackers had stolen the PII of numerous individuals in its care (the "Data Breach"). This information included, non-exhaustively, individuals' names and Social Security numbers.

7. Plaintiff bring this class action lawsuit on behalf of herself and those similarly situated to address Defendant's inadequate safeguarding of Class members' PII that they collected

and maintained; for failing to provide adequate notice to Plaintiff and other Class members that their information had been subject to the unauthorized access of an unknown criminal third party; and for failing to timely identify precisely what specific type of information was accessed.

8. Upon information and belief, Defendant maintained the PII of thousands of individuals in a negligent manner.

9. The cyberattack was carried out by the well-known cybergang, World Leaks. World Leaks can and does offer for sale unencrypted, unredacted PII to criminals. The exposed PII of Plaintiff and Class members can and likely will be sold repeatedly on the dark web.

10. Plaintiff and Class members now face a current and ongoing risk of identity theft, which is heightened here by the loss of Social Security numbers.

11. Upon information and belief, this Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class members.

12. While many details of the Data Breach remain in the exclusive control of Defendant, upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (i) failing to design, implement, monitor, and maintain reasonable software and/or network safeguards against foreseeable threats; (ii) failing to design, implement, and maintain reasonable data retention policies; (iii) failing to adequately train staff on data security; (iv) failing to comply with industry-standard data security practices; (v) failing to warn Plaintiff and Class members of Defendant's inadequate data security practices; (vi) failing to encrypt or adequately encrypt the Private Information; (vii) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (viii) failing to utilize widely available software able to detect and prevent this type of attack, and (ix) otherwise

failing to secure the software and hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

13. As a result of Defendant's unreasonable and inadequate data security practices that resulted in the Data Breach, Plaintiff's and Class members are at a current and ongoing risk of identity theft and have suffered numerous actual and concrete injuries and damages, including: (i) invasion of privacy; (ii) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their Private Information; (viii) anxiety, annoyance, and nuisance; and (ix) the continued risk to their Private Information, which remains in the control of Defendant, and which is subject to further breaches, as long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' Private Information.

14. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, future costs of identity theft monitoring, injunctive relief including improvements to Defendant's data security systems, and future annual audits.

15. Accordingly, Plaintiff brings this action against Defendant seeking redress for their unlawful conduct and asserting claims for: (i) negligence; (ii) breach of third-party beneficiary contract; (iii) breach of implied contract; (iv) negligence per se; (v) unjust enrichment; and (v) declaratory judgment.

II. THE PARTIES

Plaintiff

16. Plaintiff Jenni Barrette is a resident and citizen of the State of Rhode Island. Plaintiff received confirmation that her information was included in the Data Breach from multiple third-party monitoring services. The notification informed her that her information was compromised from the Freedman Healthcare Data Breach, including her name, address, phone number, and Social Security number.

Defendant

17. Defendant Freedman Healthcare, LLC is a Limited Liability Company organized under the laws of the Commonwealth of Massachusetts with its principal place of business located at 115 Middlesex Turnpike, Suite 1096, Burlington, Massachusetts 01803. Service of process is proper on John Freedman as agent located at the same address.

III. JURISDICTION AND VENUE

18. This Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Defendant—as evidenced by the fact that Defendant provides services to the states of Colorado, Connecticut, Rhode Island, Hawaii, Ohio, and Tennessee, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

19. This Court has personal jurisdiction over the Defendant named in this action because Defendant is headquartered in this District and Defendant conducts substantial business in Massachusetts and this District through its headquarters, offices, parents, and affiliates.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover,

Defendant Freedman Healthcare is based in this District, Defendant interacted with clients in this District, and the harm caused to Plaintiff and Class members emanated from this District.

IV. FACTUAL ALLEGATIONS

A. Freedman Healthcare's Business

21. Freedman Healthcare, which is based in Burlington, Massachusetts, is a software company that offers a wide range of products and services to government agencies. This software assists states in servicing Medicaid claims, healthcare services, and payments for public programs.

22. As a condition of receiving software services, Freedman Healthcare requires that its government customers entrust it with highly sensitive Private Information belonging to Plaintiff and Class members.

23. Because of the highly sensitive nature of the Private Information that Freedman Healthcare acquires, maintains, and transfers, Freedman Healthcare guarantees file security and promises, among other things, to: keep customers' files private; comply with industry standards related to data security and maintenance of its customers' files and the Private Information contained therein; only disclose the sensitive information for business purposes and reasons related to the services it provides; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

24. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, Freedman Healthcare assumed legal and equitable duties and knew or should have known that it was responsible for ensuring the security of Plaintiff's and Class members' Private Information to protect it from unauthorized disclosure and exfiltration.

25. Plaintiff and Class members relied on Freedman Healthcare to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Freedman Healthcare failed to do.

B. The Data Breach

26. In or around April of 2025, Freedman Healthcare discovered that cybercriminals had exfiltrated highly-sensitive PII that it stored.

27. Freedman Healthcare began notifying impacted individuals in May of 2025.

28. The cyber gang World Leaks took responsibility for the attack.

29. Defendant negligently maintained Plaintiff's and Class members' Private Information, which allowed unauthorized cybercriminals to access and exfiltrate the Private Information through the Data Breach, including, but not limited to, full names and Social Security numbers.

30. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class members financial institutions to keep Plaintiff and Class members' Private Information confidential and to protect them from unauthorized access and disclosure.

31. Plaintiff and Class members permitted their Private Information to be provided to Defendant with the reasonable expectation and understanding that Defendant would comply with its obligations to keep said Private Information confidential and secure from unauthorized access and timely notify Class members of any security breaches.

32. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years, including recent similar attacks against secure file transfer companies such as Accellion and Fortra.

33. Therefore, because of the type of data and Private Information maintained, Defendant knew or should have known that their systems and the records would be targeted by cybercriminals.

C. Freedman Healthcare Failed to Comply with FTC Guidelines

34. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

35. 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.

36. 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 their network's vulnerabilities; and implement policies to correct any security problems.[1] 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

[1] *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 Jan. 19, 2022).

the system; and have a response plan ready in the event of a breach.[2]

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

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the 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.

39. Defendant failed to properly implement data security practices.

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

41. Defendant was at all times fully aware of the obligation to protect the Private Information of customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Defendant Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

42. In addition to its obligations under federal and state laws, Defendant owed a duty

[2] *Id*.

to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

43. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

44. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

45. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

46. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

47. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

48. Defendant owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach.

49. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data.

50. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

51. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

52. However, due to Defendant's failures, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

E. Plaintiff's Experience

Plaintiff Barrette

53. Defendant received Plaintiff Barrette's PII in connection with her acquiring healthcare services. In requesting and maintaining Plaintiff's PII for business purposes, Defendant expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Barrette's PII. Defendant, however, did not take proper care of Plaintiff's PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Defendant's inadequate data security measures.

54. On or around June 14, 2025, Plaintiff Barrette's information was confirmed on the dark web. This confirmation notes that her Social Security number, among other information, is on the dark web.

55. Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff significant injuries and harm, including but not limited to, the following—Plaintiff immediately devoted (and must continue to devote) time, energy, and money to: closely monitoring their

financial statements, bills, records, and credit and financial accounts; changing login and password information; more carefully screening and scrutinizing phone calls, emails, and other communications to ensure that she is not being targeted.

56. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff will need to maintain these heightened measures for years, and possibly their entire lives. Consumer victims of data breaches are more likely to become victims of identity fraud.[3]

57. These harms have already started to manifest. Plaintiff has recently experienced multiple unauthorized charges on her credit card.

58. Plaintiff greatly values her privacy. Plaintiff and Class Members did not receive the full benefit of their bargain when using their accounts, and instead received services that were of a diminished value to those described in their agreements for the respective services that they received, including the failure of Defendant to provide the benefit and protection to Plaintiff and Class Members and their respective Private Information. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

F. The Data Breach Was Foreseeable and Preventable

71. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some

[3] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed November 30, 2022).

of the biggest cybersecurity breaches: Target,[4] Yahoo,[5] Marriott International,[6] Chipotle, Chili's, Arby's,[7] and others.[8]

72. Defendant should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

73. Defendant was clearly aware of the risks it was taking and the harm that could result from inadequate data security, and it could have prevented this Data Breach.

74. Data disclosures and data breaches are preventable.[9] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[10] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[11]

---

[4] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[5] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[6] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

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

[8] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[9] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[10] *Id.* at 17.

[11] *Id.* at 28.

75. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[12]

76. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[13] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

77. Upon information and belief, Defendant failed to follow reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines.

78. Upon information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special

[12] *Id.*
[13] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

79. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[14]

80. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

[14] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[15]

81. The threat continues. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for consumers' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).

[15] *Id.* at 3-4.

82. Further, to prevent and detect ransomware attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to

reduce malicious network traffic….[16]

G. The Monetary Value of Privacy Protections and Private Information

83. The fact that Plaintiff's and Class Members' Private Information was stolen means that Class Members' information is likely for sale by cybercriminals and will be misused in additional instances in the future. Indeed, there is already evidence that Plaintiff's Private Information is on the dark web.

84. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

85. As discussed above, Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[17]

86. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[18]

---

[16] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

[17] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed November 30, 2022). Attached hereto at Exhibit 13.

18 *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last accessed November 30, 2022). Attached hereto at Exhibit 14.

87. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[19]

88. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[20]

89. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[21] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

90. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their

---

[19] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), https://allthingsd.com/20110228/webs-hot-new-commodity-privacy/ [hereinafter *Web's New Hot Commodity*] (last accessed November 30, 2022). Attached hereto at Exhibit 15.

[20] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last accessed November 30, 2022). Attached hereto at Exhibit 16.

[21] *Web's Hot New Commodity*, *supra* note 17.

data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[22]

91. As discussed above, the value of Plaintiff's and Class Members' Private Information on the black market is substantial.

92. The ramifications of Defendant's failure to keep its patients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

93. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

94. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[23] For example, different PII and PHI elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[24] Based upon information and belief, the

[22] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*] (last accessed November 30, 2022). Attached hereto at Exhibit 17.

[23] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework (last accessed November 30, 2022). Attached hereto at Exhibit 22.

[24] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class Members that was misused.

95. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

96. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information was not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs. Here, payment card information is involved, which grants access to further harm.

97. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

98. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiff's and Class members' Private Information as detailed above, and Plaintiff and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

99. Plaintiff is also at a continued risk of harm because her PII remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are

subject to further attack so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII and in its possession.

100. As a result of the Data Breach, and in addition to the time Plaintiff has spent and anticipates spending to mitigate the impact of the Data Breach on their lives, Plaintiff has also suffered emotional distress from the public release of her PII, which she believed would be protected from unauthorized access and disclosure. The emotional distress she has experienced includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing her PII and for the purposes of identity theft and fraud.

101. Additionally, Plaintiff has suffered damage to and diminution in the value of her highly sensitive and confidential PII —a form of property that Plaintiff entrusted to Defendant and which was compromised as a result of the Data Breach Defendant failed to prevent. Plaintiff has also suffered a violation of her privacy rights as a result of Defendant's unauthorized disclosure of their PII.

102. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

103. Some of the injuries and risks associated with the loss of Private Information have already manifested themselves in Plaintiff and other Class Members' lives, including the time Plaintiff has spent to reconcile financial accounts and fight fraud attempts.

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

CLASS ACTION ALLEGATIONS

105. Plaintiff bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

106. Plaintiff propose the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals residing in the United States whose Private Information was compromised as a result of the Data Breach of Defendant's network occurring in or around April of 2025 (the "Class").

107. Excluded from the Class are Defendant's officers, directors, and agents; any entity in which Defendant has 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.

108. Plaintiff reserves the right to amend or modify the Class or Class definitions as this case progresses.

109. **Numerosity, Fed. R. Civ. P. 23(a)(1):** 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 Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose PII was stored in Defendant's systems and was compromised in Data Breach.

110. **Commonality, Fed. R. Civ. P. 23(a)(2):** 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 Plaintiff's 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's data security systems prior to and during the Data Breach were consistent with industry standards;

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

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

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

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

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

j. Whether Defendant's conduct was negligent;

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

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

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

111. **Typicality, Fed. R. Civ. P. 23(a)(3)**: Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

112. **Adequacy, Fed. R. Civ. P. 23(a)(4)**: Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

113. **Predominance, Fed. R. Civ. P. 23(b)(3)**: Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's 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.

114. **Superiority, Fed. R. Civ. P. 23(b)(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. 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.

115. 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.

116. Likewise, particular issues 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 and adequately notify the public of the Data Breach;

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

c. Whether Defendant's security measures to protect its 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.

117. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names, social security numbers, and financial information affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant's clients.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

118. Plaintiff re-alleges and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

119. Defendant knowingly collected, acquired, stored, and/or maintained Plaintiff's and Class members' PII and had a duty to exercise reasonable care in safeguarding, securing, and protecting the PII it held from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

120. The duty includes obligations to take reasonable steps to prevent disclosure of the PII, and to safeguard the information from theft. Defendant's duties included the responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

121. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the PII.

122. Defendant owed a duty of care to safeguard the PII due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to safeguard the PII.

123. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and those individuals who entrusted them with their PII, which is recognized by laws and regulations including but not limited the FTC Act, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

124. In addition, Defendant 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.

125. Defendant's duty to use reasonable care in protecting Private Information arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect Private Information that it either acquires, maintains, or stores.

126. Defendant breached their duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class members' Private Information, as alleged and discussed above.

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

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

129. The imposition of a duty of care on Defendant to safeguard the Private Information they maintained is appropriate because any social utility of Defendant's conduct is outweighed by the injuries suffered by Plaintiff and Class members as a result of the Data Breach.

130. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are at a current and ongoing risk of identity theft, and Plaintiff and Class members sustained compensatory damages including: (i) invasion of privacy; (ii) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their Private Information; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to their Private Information, which remains in Defendant's control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' Private Information.

131. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

132. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class members in an unsafe and unsecure manner.

133. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant 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
Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Class)

134. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

135. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

136. Defendant breached its duties to Plaintiff and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

137. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

138. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

139. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

140. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are at a current and ongoing risk of identity theft, and Plaintiff and Class members sustained compensatory damages including: (i) invasion of privacy; (ii) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of

time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their Private Information; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to their Private Information, which remains in Defendant's control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' Private Information.

141. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

142. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

143. Freedman Healthcare acquired and maintained Private Information belonging to Plaintiff and Class members that it received either directly or from its customers, including healthcare providers and banks.

144. When Plaintiff and Class members paid money and provided their Private Information for the provision of services, including healthcare providers, either directly or indirectly, they entered into implied contracts, including with Freedman Healthcare.

145. Plaintiff and Class members entered into implied contracts with Freedman Healthcare under which Freedman Healthcare agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their Private Information had been breached, accessed by an unknown and unauthorized party, and exposed on a hacking forum.

146. Plaintiff and Class members were required to indirectly deliver their Private Information to Freedman Healthcare as part of the process of obtaining services provided by Defendant. Plaintiff and Class members paid money, or money was paid on their behalf, to Freedman Healthcare in exchange for services.

147. Freedman Healthcare accepted possession of Plaintiff's and Class members' Private Information for the purpose of indirectly providing services to Plaintiff and Class members.

148. In accepting such information and payment for services, Freedman Healthcare entered into an implied contract with Plaintiff and the other Class members in which Freedman Healthcare became obligated to reasonably safeguard Plaintiff's and the other Class members' Private Information.

149. Freedman Healthcare's implied promise of confidentiality includes consideration beyond those preexisting general duties owed under HIPAA, the FTC Act, or other state of federal regulations. The additional consideration also included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

150. Freedman Healthcare's 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 their agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to authorized, qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the Private Information against data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

151. Plaintiff and the Class members would not have entrusted their Private Information to Freedman Healthcare in the absence of such an implied contract.

152. Had Freedman Healthcare disclosed to Plaintiff and Class members that Freedman Healthcare did not have adequate computer systems, information technology security tools, and security practices to secure sensitive data, Plaintiff and the other Class members would not have provided their Private Information to Freedman Healthcare's.

153. Freedman Healthcare recognized that Plaintiff's 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 Plaintiff and to the other Class members.

154. Plaintiff and the other Class members fully performed their obligations under the implied contracts with Freedman Healthcare. Freedman Healthcare breached the implied contract with Plaintiff and the other Class members by failing to take reasonable measures to safeguard their Private Information as described herein.

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

COUNT IV
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Nationwide Class)

156. Plaintiff re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

157. Upon information and belief, Freedman Healthcare entered into contracts with its government and corporate customers to provide secure file transfer services to them; services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

158. Upon information and belief, Freedman Healthcare entered into contracts with its government and corporate customers to provide beneficiary search services; services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

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

160. Defendant knew or should have known that if it were to breach these contracts with its customers, Plaintiff and Class members would be harmed.

161. Defendant breached its contracts with customers by, among other things, failing to adequately secure Plaintiff and Class members' Private Information, and, as a result, Plaintiff and Class members were harmed by Defendant's failure to secure their Private Information.

162. As a direct and proximate result of Defendant's breach, Plaintiff and Class members are at a current and ongoing risk of identity theft, and Plaintiff and Class members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Private Information, which remains in Defendant's control,

and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' Private Information.

163. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

164. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

165. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

166. Plaintiff and Class members conferred a monetary benefit on Defendant by Defendant using Plaintiff and Class members valuable Private Information.

167. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' Private Information, which cost savings increased the profitability of the services.

168. Upon information and belief, instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

169. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

170. Defendant acquired the monetary benefit, PII, through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

171. Had Plaintiff and Class members known that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant's clients or Defendant. Plaintiff and Class members have no adequate remedy at law.

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

173. Furthermore, as a direct and proximate result of Defendant's unreasonable and inadequate data security practices, Plaintiff and Class members are at a current and ongoing risk of identity theft and have sustained incidental and consequential damages, including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their Private Information, which remains in Defendant's control, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' Private Information.

174. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

175. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

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

COUNT VI
DECLARATORY RELIEF
(On Behalf of Plaintiff and the Nationwide Class)

177. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

178. 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 granting 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 statutes described in this Complaint.

179. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

180. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect Plaintiff's and Class members' Private Information.

181. Defendant still controls the Private Information of Plaintiff and the Class members.

182. To Plaintiff's knowledge, Defendant has made no announcement that it has changed its data or security practices relating to the Private Information.

183. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

184. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Defendant's business. The risk of another such breach is real, immediate, and substantial.

185. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

186. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

187. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs. Freedman Healthcare, Plaintiff and Class members will likely continue to be subjected to

fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

188. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and Class.

189. Plaintiff and Class members seek a declaration (i) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security; and (ii) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and promptly correct any problems or issues detected by such third-party security auditors;

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

c. audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. conduct regular database scanning and security checks; and

f. routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and their counsel as Class Counsel;

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

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and,

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

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demand a trial by jury of any and all issues in this action so triable as of right.

Dated: April 10, 2026

Respectfully submitted,

/s/ Richard E. Levine

Richard E. Levine (BBO 672675)
Stanzler Levine, LLC
37 Walnut Street, Suite 200
Wellesley, MA 02481
Tel: 617-482-3198
rlevine@stanzlerlevine.com

and

Nicholas A. Migliaccio*
Jason S. Rathod*
MIGLIACCIO & RATHOD, LLP
412 H Street, NE, Suite 302
Washington, DC 20002
Phone: 202-470-520
Fax: 202-800-2730
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Counsel for Plaintiff and Proposed Class
*To apply for admission *pro hac vice*