Exhibit A1

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

CHERYL COVINGTON, individually, and on behalf of all others similarly situated,	)	
Plaintiff	)	
V.	)	**Case No. 1:22-cv-04000-VMC**
GIFTED NURSES, LLC d/b/a GIFTED HEALTHCARE	)	
Defendant	)	

AMENDED COMPLAINT—CLASS ACTION

Plaintiff, CHERYL COVINGTON ("Plaintiff" or "Covington"), individually and on behalf of all others similarly situated, complains and alleges as follows against Defendant, GIFTED NURSES, LLC d/b/a GIFTED HEALTHCARE ("Defendant" or "Gifted Healthcare") based on personal knowledge, on the investigation of her counsel, and on information and belief as to all other matters:

INTRODUCTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant Gifted Healthcare, arising from its failure to

safeguard certain Personally Identifying Information[1] ("PII") and other sensitive, non-public financial information (collectively, "Personal Information") of thousands of its prospective, current, and former employees, resulting in Defendant's email systems being unauthorizedly accessed from August 25, 2021 to December 10, 2021 and the Personal Information of employees therein, including of Plaintiff and the proposed Class Members, being disclosed, stolen, compromised, and misused, causing widespread and continuing injury and damages.

2. On information and belief, from August 25, 2021 to December 10, 2021, Gifted Healthcare's employee email account systems were "hacked" and unauthorizedly accessed, resulting in the unauthorized disclosure of the Personal Information of Plaintiff and the Class Members, including names, Social Security Numbers,[2] PII, and financial account information and numbers

[1] The Federal Trade Commission defines "personally identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the breach.

[2] *See:* Gifted Healthcare Notice of Data Breach to Plaintiff Covington, August 24, 2022, attached as **Exhibit A**; and, Gifted Healthcare sample Notice of Data Breach to Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/3be2682e-fc94-4330-9047-

(the "Data Breach").[3]

3. On information and belief, approximately 13,770 persons were impacted by the Data Breach.[4]

4. As explained below, Plaintiff and Members of the Class have suffered significant injury and damages due to the Data Breach permitted to occur by Gifted Healthcare, and the resulting misuse of their Personal Information and fraudulent activity, including fraudulent attempts to open bank accounts, decreased credit scores, monetary damages including out-of-pocket expenses, including those associated with the reasonable mitigation measures they were forced to employ, and other damages. Plaintiff and the Class also now forever face an amplified risk of *further* misuse, fraud, and identity theft due to their sensitive Personal Information falling into the hands of cybercriminals as a result of the tortious conduct of Defendant.

5. On behalf of herself and the Class preliminarily defined below, Plaintiff brings causes of action for negligence, negligence *per se*, breach of implied contractual duty, breach of express contract, and unjust enrichment.

---

d50d61d81cf7/221d5f8a-742d-491f-8048-fd13174693b1/document.html (last accessed September 17, 2022).

[3] *Id.*

[4] Gifted Healthcare report to Maine Attorney General, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/3be2682e-fc94-4330-9047-d50d61d81cf7.shtml (last accessed September 17, 2022).

Plaintiff seeks damages and injunctive and declaratory relief arising from Gifted Healthcare's failure to adequately protect her highly sensitive Personal Information.

PARTIES

6. Plaintiff Covington is a natural person and citizen of the state of Georgia, residing in Conyers, Georgia, in the County of Rockdale, where she intends to remain. Covington is a former employee of Gifted Healthcare.

7. Defendant, Gifted Nurses, LLC d/b/a Gifted Healthcare is a limited liability company organized and existing under the laws of the state of Louisiana, with a principal place of business located at 3330 W. Esplanade Avenue, Suite 505, Metairie, Louisiana 70002.

8. Gifted Healthcare is a nationwide staffing company which employs persons in the nursing profession across the United States in the healthcare field, including local, per diem, and "PRN" nurses, as well as travel nurses.[5] As Defendant has stated:

> GIFTED offers nurses the option to work Local Contracts, LTAC contracts, Per Diem Nursing shifts, Travel Nursing assignments, or Government Nursing contracts. GIFTED also offers Infusion Nursing, in which nurses work one-on-one with employees in their

[5] *See* Gifted Healthcare website, available at https://www.giftedhealthcare.com/ (last accessed September 17, 2022).

setting providing infusion therapy.[6]

9. Gifted Healthcare represents that it "provides nurses with the exceptional experiences and steadfast support they deserve"[7] in these services.

10. Gifted Healthcare's nursing employees work throughout the United States, in Texas, California, Florida, Tennessee, Virginia, Ohio, Louisiana, Arizona, Georgia, Oklahoma, Missouri, South Carolina, Colorado, Pennsylvania, New Mexico, Kentucky, North Carolina, Wisconsin, Indiana, Kansas, Washington, Oregon, Arkansas, Iowa, Mississippi, Alabama, Alaska, North Dakota, New Hampshire, New York, Nebraska, Connecticut, Utah, Montana, New Jersey, Vermont, Wyoming, Idaho, and in Maine.[8]

11. Since 2017, Gifted Healthcare's nursing services were expanded to Georgia.[9]

12. Gifted Healthcare has "top per diem nursing shifts and convenient local contract nursing opportunities that fit your lifestyle and meet you where

---

[6] Gifted Healthcare website, "GIFTED Announces Service Line Expansion in Georgia" available at https://www.giftedhealthcare.com/gifted-announces-service-line-expansion-in-georgia/

[7] Gifted Healthcare website, "Our Story" available at https://www.giftedhealthcare.com/our-story/ (last accessed September 17, 2022).

[8] See Gifted Healthcare website, "Job Search" available at https://www.giftedhealthcare.com/job-search/ (last accessed September 17, 2022).

[9] Gifted Healthcare website, "GIFTED Announces Service Line Expansion in Georgia" available at https://www.giftedhealthcare.com/gifted-announces-service-line-expansion-in-georgia/ (last accessed September 17, 2022).

you are…" and represents that it "remain[s] committed to keeping talented nurses like you at the bedside - in your backyard or across the country."[10]

13. Gifted Healthcare also holds itself out as "an award-winning travel nursing agency that offers nursing contracts at premier healthcare facilities across the United States"[11] and is "…recognized by global experts Staffing Industry Analysts (SIA) on the list of the Largest US Travel Nurse Staffing Firms."[12]

14. In addition, Gifted Healthcare contracts to provide its nursing employees to governmental entities, including the U.S. Air Force, the Veterans Administration, Indian Health Service Centers, and the U.S. Bureau of Prison Clinics.[13]

JURISDICTION AND VENUE

15. Jurisdiction is proper in this Court pursuant to the Class Action

---

[10] Gifted Healthcare website, "Local PRN" available at https://www.giftedhealthcare.com/local-prn/ (last accessed September 17, 2022).

[11] Gifted Healthcare website, "Travel Nursing," available at https://www.giftedhealthcare.com/travel-nursing/ (last accessed September 17, 2022).

[12] Gifted Healthcare website, "Gifted Healthcare Named Among the 2022 Largest Staffing Firms," available at https://www.giftedhealthcare.com/gifted-healthcare-named-among-the-2022-largest-us-staffing-firms/ (last accessed September 17, 2022).

[13] Gifted Healthcare website, "Government Contracting," avail. at https://www.giftedhealthcare.com/government-contracting-2/ (last accessed September 17, 2022).

Fairness Act, 28 U.S.C. § 1332(d), because: (i) there are more than one hundred (100) Class Members; (ii) the aggregate amount in controversy exceeds five million dollars ($5,000,000.00), exclusive of interest and costs; and (iii) some Class Members are citizens of states different than Gifted Healthcare.

16. This Court has personal jurisdiction over Gifted Healthcare because it regularly and systematically transacts business in the State of Georgia, such that it can reasonably anticipate defending a lawsuit here. Moreover, this Court has jurisdiction over Defendant because its acts and omissions effected Plaintiff's property interests within the state of Georgia.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to these claims occurred in this district, and/or or a substantial part of property that is the subject of this action is situated herein.

FACTUAL ALLEGATIONS

A. Plaintiff and the Class Members entrusted their Personal Information to Gifted Healthcare

18. Plaintiff Covington and the Members of the proposed Class are present and former employees and prospective employees of Gifted Healthcare.

19. From November 2014 to August 2018, Covington was an employee of Gifted Healthcare in Oklahoma City, Oklahoma as a Certified Nursing

Assistant (CNA), at 2610 NW Expressway, Suite C, Oklahoma City, Oklahoma.

20. As a condition of employment, and/or of applying for employment with Gifted Healthcare, Plaintiff and the Class Members were required by Gifted Healthcare to confide and make available to it their sensitive and confidential Personal Information, including, but not limited to, their PII, names and Social Security Numbers, as well as financial information, bank routing number, and account number.

21. On information and belief, Plaintiff believed there was a privacy policy under which Defendant would protect her Personal Information based on her past experiences when submitting an application for contract nursing through agencies.

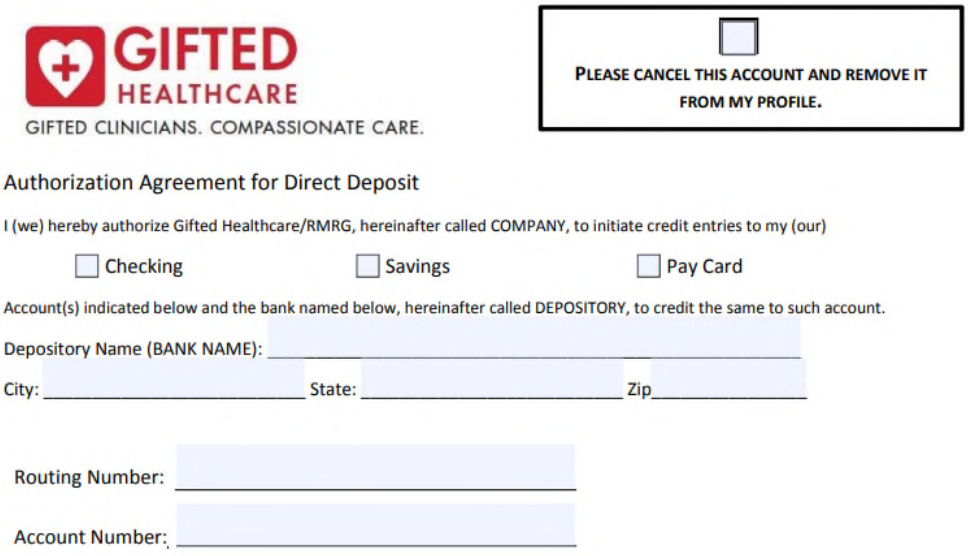
22. Gifted Healthcare required that prospective employees apply for employment online, through an online application portal, the "Workforce Portal",[14] and to provide their Personal Information therein.

23. Gifted Healthcare required Plaintiff and the Class Members to receive renumeration by direct deposit into their checking and/or savings

[14] *See* Gifted Healthcare Workforce Portal, avail. at https://ctms.contingenttalentmanagement.com/giftednurses/WorkforcePortal/login.cfm (last accessed September 17, 2022).

accounts, or Gifted Healthcare "Pay Card" accounts.

24. In order for Plaintiff and the Class Members to receive payment via direct deposit, Gifted Healthcare required them to provide their Personal Information including depository institution names, routing numbers, and financial account numbers, via an "Authorization Agreement for Direct Deposit" form, ("Authorization Agreement"), authorizing Defendant to "…initiate credit entries" to their depository accounts and/or a Gifted Healthcare Pay Card, reproduced in part below:[15]



GIFTED HEALTHCARE
GIFTED CLINICIANS. COMPASSIONATE CARE.

☐ PLEASE CANCEL THIS ACCOUNT AND REMOVE IT FROM MY PROFILE.

Authorization Agreement for Direct Deposit

I (we) hereby authorize Gifted Healthcare/RMRG, hereinafter called COMPANY, to initiate credit entries to my (our)

☐ Checking ☐ Savings ☐ Pay Card

Account(s) indicated below and the bank named below, hereinafter called DEPOSITORY, to credit the same to such account.

Depository Name (BANK NAME): _____

City: _____ State: _____ Zip_____

Routing Number: _____

Account Number: _____

25. To receive compensation, Gifted Healthcare further required

[15] *See* Gifted Healthcare website, avail. at https://www.giftedhealthcare.com/wp-content/uploads/2022/02/Direct-Deposit-Form-2018.pdf (last accessed September 17, 2022).

Plaintiff and the Class Members to provide Defendant with a voided check.[16]

26. Gifted Healthcare's Authorization Agreement provided that: "[t]his authority is to remain in full force and effect until COMPANY has received written notification from me (us) of its termination in such time and in such manner as to afford COMPANY and DEPOSITORY a reasonable opportunity to act on it."[17]

27. Covington and the Class Members executed the Authorization Agreement, providing their Personal Information including financial information to Gifted Healthcare to receive renumeration via direct deposit into their financial accounts and/or on a Pay Card.

28. In addition, Gifted Healthcare required employees, Covington and the Class Members, to provide Defendant with their Personal Information and account numbers on Defendant's "Weekly Time Sheets".[18]

29. Moreover, Gifted Healthcare received employee Personal Information through the "Workforce Portal."[19]

---

[16] *Id.*
[17] *Id.*
[18] *See* Gifted Healthcare website, available at https://www.giftedhealthcare.com/wp-content/uploads/2022/02/Local-Assignment-Weekly-Time-Sheet-4-19-2021.pdf (last accessed September 17, 2022).
[19] *See* Gifted Healthcare website, "Workforce Portal," avail. at https://ctms.contingenttalentmanagement.com/giftednurses/WorkforcePortal/login.cfm (last accessed September 17, 2022).

30. The Data Breach that is the subject of this civil action is not contemplated or permitted by Gifted Healthcare's Authorization Agreement or weekly Time Sheets.

31. Gifted Healthcare acquired, collected, and stored a massive amount of said Personal Information of its employees, including Covington and the Members of the proposed Class, which it stored in its electronic systems.

32. By obtaining, collecting, using, and deriving a benefit from its employees' Personal Information, Gifted Healthcare assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their Personal Information from unauthorized disclosure.

33. Plaintiff has taken reasonable steps to maintain the confidentiality of her Personal Information. Plaintiff, as a former employee, relied on Gifted Healthcare to keep her Personal Information confidential and securely maintained, to use this information for authorized purposes and disclosures only.

34. Covington has never been the victim of another data breach.

35. In addition, Gifted Healthcare maintains a Privacy Policy

applicable to use of its website, which "describes how [it] processes, collects, uses and discloses personal information when using this website https://www.giftedhealthcare.com (the 'Site')."[20]

36. Gifted Healthcare's Privacy Policy defines "personal information" as:

> information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. **This includes various categories of information about you, including, but not limited to, your name, postal address, email address,** telephone number, IP address, location data, professional or employment-related information, education information, preferences, and characteristics.[21] (emphasis added)

37. In its Privacy Policy, Gifted Healthcare represents that it needs said personal information to provide visitors to its website with website services, and promises to "only process your personal information in accordance with applicable data protection and privacy laws."[22]

38. Gifted Healthcare's Privacy Policy further states that it collects Personal Information in the following ways:

- information you provide when you submit an application on our Site, including your name, zip code, email address, telephone number, profession, specialty, referral information, job preferences, and

[20] Gifted Healthcare website, "Privacy Policy," https://www.giftedhealthcare.com/privacy-policy/ (last accessed August 1, 2023).
[21] *Id.*
[22] *Id.*

resumé;

- information you provide when you interact with us via our Site's live chat feature;
- information you provide when you report a problem with our Site or when we provide you with customer support;
- information you provide when you request nursing services through our Site, including your name, email address, telephone number, the nursing services of interest to you, and any additional information you may provide;
- information you provide when you search for jobs or sign up for a career consultation on our Site, including your name, email address, telephone number, job preference, current city and state, profession, and information about your values, preferences, and personality;
- information you provide when you subscribe to our newsletter, including your email address; and
- information you provide when you correspond with us by phone, email or otherwise.[23]

39. Defendant's Privacy Policy provides that Gifted Healthcare may use Personal Information for limited purposes:

- to operate, maintain, and improve our Site, products, and services, including engaging in communications, services, advertising, marketing activities, and data analysis; auditing and assessing quality and safety; monitoring and preventing fraud, infringement, and other potential misuse of the Services; determining the effectiveness of our promotional campaigns; improving our services and technology; and operating and expanding our business activities;
- to process, complete and fulfill your requested transactions, or provide our services;
- to manage your account, including to communicate with you regarding your account, if you have an account on our Site;

[23] *Id.*

- to understand how you and other users interact with our online services through our Site, using online tools such as Google Analytics;
- to better understand our audiences, evaluate user interest in the Services, and perform other market research activities;
- to operate our referral program;
- to respond to your comments and questions, provide customer service, verify information provided to us, and determine eligibility for our services;
- to send you information including technical notices, updates, security alerts, and support and administrative messages;
- to send you marketing emails and other news, including information about products and services offered by us and our affiliates. You may opt-out of receiving such information at any time by clicking the "Unsubscribe" link at the bottom of all such marketing emails;
- as necessary or appropriate under applicable law, including laws outside your country of residence, to meet legal and regulatory requirements, and comply with legal process; respond to requests from public and government authorities, including those outside your country of residence; enforce our Terms and Conditions; protect our operations or those of any of our affiliates; protect our rights, privacy, safety or property, and/or those of our affiliates, you or others; allow us to pursue available remedies or limit the damages that we may sustain, and protect against fraud, suspicious or other illegal activities.[24]

40. In its Privacy Policy, Gifted Healthcare promises that it will not sell Personal Information to third parties for business or commercial purposes, and that it will disclose Personal Information as described in the policy or in any other applicable privacy notices or opt-ins that website visitors may

[24] *Id.*

receive; that Gifted Healthcare will disclose Personal Information to third parties with consent; to service providers; for business transfers or assignments; to third parties for limited purposes; and as required by law.[25]

41. Further, in its Privacy Policy, Gifted promised that it will "use reasonable organizational, technical and administrative measures to protect personal information within our organization."[26]

42. The Data Breach that is the subject of this civil action is not contemplated or permitted by Gifted Healthcare's website Privacy Policy.

43. Plaintiff and the proposed Class Members entrusted their Personal Information to Gifted Healthcare solely for the purposes of applying for employment with Defendant and/or as a condition of employment, with the expectation and implied mutual understanding that Gifted Healthcare would strictly maintain the confidentiality of the information and undertake adequate measures to safeguard it from theft or misuse.

44. Plaintiff and the proposed Class Members would not have entrusted Gifted Healthcare with their highly sensitive Personal Information if they had known that Gifted Healthcare would fail to take adequate measures

[25] *See id.*
[26] *Id.*

to protect it from unauthorized use or disclosure.

B. Plaintiff's and the Class Members' Personal Information was Unauthorizedly Disclosed and Compromised in the Data Breach

45. As stated prior, Plaintiff Covington applied for employment with Gifted Healthcare and was employed by Defendant for years from November 2014 to August 2018.

46. As a prerequisite to employment, Plaintiff and the Class Members disclosed their non-public and sensitive Personal Information to Gifted Healthcare, with the implicit understanding that their Personal Information would be kept confidential. This understanding was based on all the facts and circumstances attendant to their employment there, and the express, specific, written representations made by Gifted Healthcare and its agents.

47. Plaintiff and the Class Members reasonably relied upon Gifted Healthcare's representations to her detriment and would not have provided their sensitive Personal Information to Gifted Healthcare if not for Gifted Healthcare's explicit and implicit promises to adequately safeguard that information.

48. In August 2021, Covington moved from Oklahoma City, where she had worked for Defendant, to Georgia.

49. On or about August 24, 2022, Gifted Healthcare began sending

letters to the Class Members notifying them that their Personal Information had been compromised during the Data Breach ("Notice").[27] Covington received the Notice during the week of September 5, 2022. *See* Exhibit A.

50. According to Gifted Healthcare's Notice, Defendant had "recently learned of suspicious activity related to an employee email account," after which it "took swift action to secure [its] email system and network," employed cybersecurity specialists, and conducted an investigation which revealed that three (3) employee email accounts were unauthorizedly accessed between August 25, 2021 and December 10, 2021.[28]

51. Defendant further represented that it had implemented additional technical safeguards to enhance the security of information in its possession and prevent similar incidents from happening in the future.[29]

52. According to Gifted Healthcare, it then reviewed the "entire mailbox contents in order to identify what information was impacted," which was completed on July 25, 2022, revealing that affected persons' names, Social Security Numbers, and other information including financial bank routing and account numbers, were unauthorizedly accessed in the Data Breach.[30]

---

[27] *See* Notice of Data Breach, August 24, 2022 (Exhibit A)
[28] *Id.*
[29] *Id.*
[30] *Id.*

53. Gifted Healthcare urged those affected by the Data Breach to remain vigilant in regularly reviewing and monitoring their accounts and explanation of benefits statements, and to contact the financial institution or company if any "suspicious activity" was discovered.[31]

54. In addition, Gifted Healthcare's Notice provided a toll-free telephone number for affected persons receiving the Notice to call for their questions to be addressed.[32]

55. Despite Gifted Healthcare claiming in its Notice that it had no reason to believe any impacted information had been misused, it offered complimentary credit monitoring and identity protection services through Equifax Credit Watch Gold.

56. As a result of this Data Breach, the Personal Information of Plaintiff and the proposed Class Members, believed to approximate 13,770 individuals, was unauthorizedly disclosed and compromised in the Data Breach.

57. The Data Breach was preventable and a direct result of Gifted Healthcare's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect employees' Personal

[31] *Id.*
[32] *Id.*

Information.

58. In addition, while Gifted Healthcare allegedly discovered the Data Breach on July 25, 2022, as reported to the Maine Attorney General, it is clear from Defendant's Notice that the breach was discovered long before, and that an investigation was instituted, but that it failed to notify affected persons in a timely manner until late August 24, 2022.[33]

C. The healthcare industry is a prime target for cybercriminals

59. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[34] The next year, that number increased by nearly 50%.[35] The following year the healthcare sector was the second easiest "mark" among all major sectors and categorically had the most widespread exposure per data breach.[36]

---

[33] Gifted Healthcare Report to Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/3be2682e-fc94-4330-9047-d50d61d81cf7.shtml (last accessed September 17, 2022).

[34] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER ("ITRC") (Jan. 19, 2017), https://www.idtheftcenter.org/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout/.

[35] *2017 Annual Data Breach Year-End Review*, ITRC, (Jan. 25, 2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

[36] *2018 End-of-Year Data Breach Report*, ITRC, (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

60. The Personal Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach— most notably names and Social Security Numbers —is difficult, if not impossible, to change.

61. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information… [is] worth more than 10x on the black market."[37]

62. PII data for sale is so valuable because PII is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining PII with false provider numbers to file fake claims with insurers.

63. The value of Plaintiff's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post

[37] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

64. Email phishing schemes "remain[] the primary attack vector for nine out of 10 cyberattacks."[38] Gifted Healthcare did not elaborate on how the Data Breach happened, other than that three (3) employee email accounts were hacked.[39] Since "91% of ransomware attacks are the result of phishing exploits…" in the healthcare sector, it is more than plausible that the Data Breach was due to a phishing attack too.[40]

65. Companies can mount two primary defenses to phishing scams: employee education and technical security barriers.

66. Employee education is the process of adequately making employees aware of common phishing attacks and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. Employee

---

[38] Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH, (Apr. 4, 2019), https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

[39] *See* n.32, *supra*.

[40] *Security Report Health Care – Hospitals, Providers and more*, CORVUS INSURANCE 2 (Mar. 3, 2020), https://info.corvusinsurance.com/hubfs/Security%20Report%202.2%20-%20Health%20Care%20.pdf.

education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and preventing unauthorized access to PII.

67. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send emails on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

D. Gifted Healthcare failed to sufficiently protect the Personal Information that Plaintiff and the Proposed Class Members Had Entrusted to It.

i. Gifted Healthcare failed to adhere to FTC guidelines

68. According to the Federal Trade Commission("FTC"), the need for data security should be factored into all business decision-making.[41] To that end, the FTC has issued numerous guidelines identifying best data security

[41] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Sep. 2, 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

practices that businesses, such as Gifted Healthcare, should employ to protect against the unlawful exposure of Personal Information.

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[42] The guidelines explain that businesses should:

a. protect the personal information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

70. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data;

[42] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Sep. 28, 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

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.[43]

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, 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.

72. Gifted Healthcare's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

ii. Gifted Healthcare failed to adhere to industry standards

73. As stated above, the healthcare industry continues to be a high value target among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data breaches, a number which continued to grow in 2018

[43] *See Start with Security*, *supra* n.40.

(363 breaches).[44] The costs of healthcare data breaches are among the highest across all industries, topping $380 per stolen record in 2017 as compared to the global average of $141 per record.[45] As a result, both the government and private sector have developed industry best standards to address this growing problem.

74. The United States Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that, "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[46] DHHS highlights "several basic cybersecurity safeguards that can be implemented to improve cyber resilience which only require a relatively small financial investment, yet they can have a major impact on an organization's cybersecurity posture."[47] Most notably, organizations must properly encrypt

---

[44] 2018 End of Year Data Brach Report, ITRC, (Feb. 20, 2019), https://www.idtheftcenter.org/ wp-content/uploads/2019/02/ITRC_2018-End-of-Year Aftermath_FINAL_V2_ combinedWEB.pdf.
[45] *Ibid.*
[46] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.
[47] *Id.*

PII in order to mitigate against misuse.

75. The private sector has similarly identified the healthcare sector as particularly vulnerable to cyber-attacks both because of the of value of the PII that it maintains and because, as an industry, it has been slow to adapt and respond to cybersecurity threats.[48]

76. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Gifted Healthcare failed to adopt sufficient data security processes, a fact highlighted in Gifted Healthcare's Notice to affected persons in which it revealed that only after the Data Breach did it implement "additional technical safeguards to enhance the security of information in its possession."[49]

77. Gifted Healthcare failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

a. How to detect phishing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols

[48] *10 Cyber Security Best Practices For the Healthcare Industry*, NTIVA (Jun. 19, 2018), https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry.
[49] *See* n.32, *supra*.

for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information; and

e. Implementing guidelines for maintaining and communicating sensitive data.

78. Gifted Healthcare's failure to implement these rudimentary measures made it an easy target for the Data Breach that came to pass.

E. Plaintiff and the Class Members were significantly injured by the Data Breach

79. As a result of Gifted Healthcare's failure to prevent the Data Breach, Plaintiff Covington and the Class Members have suffered and will continue to suffer significant injury and damages. They have suffered or are at increased risk of suffering:

a. Misuse of Personal Information and fraudulent applications, including to open a fraudulent Wells-Fargo checking account in Ms. Covington's name;

b. Decrease in credit scores, with Covington's credit score being decreased by sixteen (16) points;

c. The loss of the opportunity to control how Plaintiff's and the Class Members' Personal Information is used;

d. The diminution in value of their Personal Information;

e. The compromise, publication and/or theft of their Personal Information;

f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services;

g. Lost opportunity costs and lost wages associated with the time and effort 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;

h. Delay in receipt of tax refund monies;

i. Unauthorized use of stolen Personal Information;

j. The continued risk to their Personal Information, which remains in the possession of Gifted Healthcare and is subject to further breaches so long as it fails to undertake

appropriate measures to protect the Personal Information in their possession; and

k. Current and future costs related to the 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.

80. As a result of the Data Breach, Plaintiff and the Class Members now face, and will continue to face, a heightened risk of identity theft and fraud for the rest of their lives.

81. As a long-standing member of the healthcare community, Gifted Healthcare knew or should have known the importance of safeguarding patient Personal Information entrusted to it and of the foreseeable consequences of a breach. Despite this knowledge, however, Gifted Healthcare failed to undertake adequate cyber-security measures to prevent the Data Breach email attack from happening.

82. Although Gifted Healthcare has offered affected victims complimentary credit monitoring and identity protection services through Equifax Credit Watch Gold, this will not adequately compensate Covington and the Class Members for the injuries and damages resulting from the Data Breach which Defendant failed to prevent.

83. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[50]

CLASS ACTION ALLEGATIONS

84. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Fed. R. Civ. Proc. 23. The Class is preliminarily defined as:

> All individuals whose Personal Information was compromised as a result of the Data Breach with Gifted Healthcare which was announced on or about August 24, 2022.

85. Excluded from the Class are Gifted Healthcare and its subsidiaries and affiliates, officers, directors, and members of their immediate families, and any entity in which it has a controlling interest, the legal representatives, heirs, successors or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

86. Plaintiff reserves the right to modify or amend the definition of the proposed Class and/or to add a subclass(es) if necessary, before this Court

[50] *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUSTICE 10, 11 (Jan. 27, 2014), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

determines whether certification is appropriate.

87. *Fed. R. Civ. Proc. 23(a)(1) Numerosity:* The Class is so numerous such that joinder of all Members is impracticable. Upon information and belief, and subject to class discovery, the Class consists of 13,770 current and former employees of Gifted Healthcare, the identity of whom are within the exclusive knowledge of and can be ascertained only by resort to Gifted Healthcare's records. Gifted Healthcare has the administrative capability through its computer systems and other records to identify all Members of the Class, and such specific information is not otherwise available to Plaintiff.

88. *Fed. R. Civ. Proc. 23(a)(2) Commonality and Fed. R. Civ. Proc. 23(b)(3) Predominance:* There are numerous questions of law and fact common to the Class. As such, there is a well-defined community of interest among the Members of the Class. These questions predominate over questions that may affect only individual Members of the Class because Gifted Healthcare has acted on grounds generally applicable to the Class. Such common legal or factual questions include, but are not limited to:

a. Whether Gifted Healthcare had a duty to protect employee Personal Information;

b. Whether Gifted Healthcare knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Gifted Healthcare's security measures to protect its systems were reasonable considering best practices recommended by data security experts;

d. Whether Gifted Healthcare was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Gifted Healthcare's failure to implement adequate data security measures allowed the Data Breach to occur;

f. Whether Gifted Healthcare's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unlawful exposure of the Plaintiff's and Class Members' Personal Information;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Gifted Healthcare's failure to reasonably protect its systems and data network;

h. Whether Plaintiff and Class Members are entitled to relief;

i. Whether Gifted Healthcare failed to adequately notify Class Members of the compromise of their Personal Information;

j. Whether Gifted Healthcare assumed a fiduciary duty and/or

confidential relationship to Class Members when they entrusted it with their Personal Information;

k. Whether Gifted Healthcare breached its contracts with Class Members by failing to properly safeguard their Personal Information and by failing to notify them of the Data Breach;

l. Whether Gifted Healthcare's violation of FTC regulations constitutes evidence of negligence or negligence *per se*;

m. Whether Gifted Healthcare impliedly warranted to Class Members that the information technology systems were fit for the purpose intended, namely the safe and secure processing of Personal Information, and whether such warranty was breached.

89. *Fed. R. Civ. Proc. 23(a)(3) Typicality:* Plaintiff's claims are typical of the claims of all Class Members, because all such claims arise from the same set of facts regarding Gifted Healthcare's failures:

a. to protect Plaintiff's and Class Members' Personal Information;

b. to discover and remediate the security breach of its computer systems more quickly; and

c. to disclose to Plaintiff and Class Members in a complete and timely manner information concerning the security breach and the theft of their Personal Information.

90. *Fed. R. Civ. Proc. 23(a)(4) Adequacy:* Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff is a more than adequate representative of the Class in that Plaintiff is a victim of the Data Breach, has suffered injury and damages such as misuse and fraudulent activity as a result of the Data Breach, and brings the same claims on behalf of herself and the putative Class. Plaintiff has no interests antagonistic to that of the Class Members. Plaintiff has retained counsel who are competent and experienced in litigating class actions, including class actions following data breaches and unauthorized data disclosures. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

91. *Fed. R. Civ. Proc. 23(b)(2) Injunctive and Declaratory Relief:* Gifted Healthcare has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

92. *Fed. R. Civ. Proc. 23(b)(3) Superiority:* It is impracticable to bring Class Members' individual claims before the Court. Class treatment permits many similarly situated persons to prosecute their common claims in a single

forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

93. A class action is superior to the other available methods for the fair and efficient adjudication of this controversy because:

a. The unnamed Members of the Class are unlikely to have an interest in individually controlling the prosecution of separate actions;

b. Concentrating the litigation of the claims in one forum is desirable;

c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

d. Plaintiff's legal counsel has the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

94. Plaintiff knows of no unique difficulty to be encountered in the

prosecution of this action that would preclude its maintenance as a class action.

95. *Fed. R. Civ. Proc. 23(c)(4) Issue Certification:* Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Gifted Healthcare owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing and safeguarding their Personal Information;

b. Whether Gifted Healthcare's security measures to protect its data systems were reasonable considering best practices recommended by data security experts;

c. Whether Gifted Healthcare's failure to institute adequate protective security measures amounted to negligence;

d. Whether Gifted Healthcare failed to take commercially reasonable steps to safeguard prospective employee and employee Personal Information; and

e. Whether adherence to FTC data security recommendations, and industry standards on data security would have

reasonably prevented the Data Breach.

96. Finally, all Members of the proposed Class are readily ascertainable. Gifted Healthcare has access to employee and applicant names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing constitutionally sufficient notice.

COUNT I
NEGLIGENCE

97. Plaintiff Covington and the Members of the Class incorporate the above allegations as if fully set forth herein.

98. Defendant Gifted Healthcare owed a duty to Plaintiff and the Members of the Class to exercise reasonable care to safeguard their Personal Information in its possession, based on the foreseeable risk of a data breach and the resulting exposure of their information, as well as on account of the special relationship between Defendant and its employees, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

99. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Members of the Class's Personal

Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

100. Further, Defendant owed to Plaintiff and Members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their Personal Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Members of the Class to take appropriate measures to protect their Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

101. Gifted Healthcare owed these duties to Plaintiff and Members of the Class because they are Members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Members of the Class's personal information and PII for employment purposes.

102. Plaintiff and Members of the Class were required to provide their Personal Information to Defendant as a condition of applying for employment and/or as a condition of employment, and Defendant retained that information.

103. The risk that unauthorized persons would attempt to gain access to the Personal Information and misuse it was foreseeable. Given that Defendant holds vast amounts of this information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Personal Information, whether by email hacking attack, or otherwise.

104. Personal Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiff and Members of the Class, and the importance of exercising reasonable care in handling it.

105. Defendant Gifted Healthcare breached its duties by failing to exercise reasonable care in supervising its employees and agents, and in handling and securing the Personal Information and PII of Plaintiff and Members of the Class which actually and proximately caused the Data Breach and Plaintiff's and Members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to

Plaintiff and Members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Members of the Class's injuries-in-fact.

106. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Members of the Class have suffered or will suffer injury and damages, including misuse and fraudulent activity, monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

107. Defendant's breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and Members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
NEGLIGENCE *PER SE*

108. Plaintiff and the Class Members incorporate the above allegations

as if fully set forth herein.

109. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' Personal Information, PII.

110. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' and prospective employees' PII.

111. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

112. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' and prospective employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had required and solicited, collected, and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to employees in the event of a breach,

which ultimately came to pass.

113. The harm that has occurred in the Data Breach is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class Members.

114. Defendant had a duty to Plaintiff and the Class Members to implement and maintain reasonable security procedures and practices to safeguard their PII.

115. Defendant breached its respective duties to Plaintiff and Members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' PII.

116. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

117. But-for Gifted Healthcare's wrongful and negligent breach of its duties owed to Plaintiff and the Class, Plaintiff and the Members of the Class would not have been injured.

118. The injury and harm suffered by Plaintiff and the Class Members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and Members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

119. Had Plaintiff and Members of the Class known that Defendant did not adequately protect employees' and prospective employees' PII, Plaintiff and Members of the Class would not have entrusted Defendant with their PII.

120. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class Members have suffered harm, injury, and damages as set forth in the preceding paragraphs.

COUNT III
BREACH OF IMPLIED CONTRACTUAL DUTY

121. Plaintiff and Members of the Class incorporate the above paragraphs 1-96 as if fully set forth herein.

122. Defendant offered to provide employment and payment to Plaintiff and Members of the Class in exchange for their labor.

123. Gifted Healthcare also required Plaintiff and the Members of the Class to provide Defendant with their Personal Information as a condition of applying for employment, and for employees as a condition of receiving

renumeration for labor rendered.

124. In turn, and through its conduct and representations, including those set forth in the Privacy Policy, which it made available on its website, Defendant agreed it would not disclose Personal Information it collects to unauthorized persons, and promised to maintain safeguards to protect their Personal Information.

125. Plaintiff and the Members of the Class accepted Defendant's offer by providing Personal Information to Gifted Healthcare, in applying for employment, and providing labor to Defendant and receiving renumeration.

126. The agreement was supported by adequate consideration, as it was an exchange of labor and Personal Information for money.

127. Implicit in the Parties' agreement was that Defendant would provide Plaintiff and Members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their Personal Information.

128. Plaintiff and the Members of the Class would not have entrusted their Personal Information to Defendant in the absence of such agreement with Defendant.

129. Gifted Healthcare materially breached the implied contract(s) it had entered with Plaintiff and Members of the Class by failing to safeguard such Personal Information and failing to notify them promptly of the intrusion

into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and Members of the Class by:

a. Failing to properly safeguard and protect Plaintiff' and Members of the Class's Personal Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic Personal Information that Defendant received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

130. The damages sustained by Plaintiff and Members of the Class as set forth in the preceding paragraphs were the direct and proximate result of Defendant's material breaches of its agreement(s).

131. Plaintiff and Members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

132. The covenant of good faith and fair dealing is implied into every contract. The parties must act with honesty in fact in the conduct or

transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

133. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

134. Defendant failed to advise Plaintiff and Members of the Class of the Data Breach promptly and sufficiently.

135. In these and other ways, Defendant violated its duty of good faith and fair dealing.

136. Plaintiff and Members of the Class have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
BREACH OF EXPRESS CONTRACT

137. Plaintiff and Members of the Class incorporate the above paragraphs 1-96 as if fully set forth herein.

138. This claim for breach of express contract is pleaded solely in the alternative to the claim for breach of implied contractual duties.

139. Defendant offered to provide employment to Plaintiff and Members of the Class, in exchange for their labor, and in exchange for their Personal Information, pursuant to the conditions set forth in written agreements, in Defendant's Privacy Policy, and in other policies and writings.

140. Plaintiff and the Class Members accepted Defendant's offer of employment in writing and provided their Personal Information and labor to Defendant.

141. The writings constituting the contract between Plaintiff and the Members of the Class and Defendant included Defendant's Privacy Policy—made available on its website and in other format—in which Defendant promised not to disclose Plaintiff's and the Members of the Class's Personal Information to unauthorized persons, and to "use reasonable organizational, technical and administrative measures to protect personal information within our organization,"[51] and, on information and belief, other written policies.

142. The parties' agreement was supported by adequate consideration, as it was an exchange of labor and Personal Information for money.

[51] https://www.giftedhealthcare.com/privacy-policy/

143. Defendant materially breached the contract it had entered into with Plaintiff and Members of the Class by failing to safeguard their Personal Information as set forth in its Privacy Policy and other writings.

144. The damages sustained by Plaintiff and Members of the Class as set forth in the preceding paragraphs were the direct and proximate result of Defendant's material breaches of its express agreement(s).

145. Plaintiff and Members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

146. Plaintiff and Members of the Class have sustained damages as a result of Defendant's breaches of its agreement.

COUNT V
UNJUST ENRICHMENT

147. Plaintiff and Members of the Class incorporate the above paragraphs 1-96 as if fully set forth herein.

148. This claim is pleaded in the alternative to the claims for breach of express contract and in the alternative to the breach of implied contractual duty claim.

149. Plaintiff and Members of the Classes conferred a benefit upon Defendant in the form of labor rendered in exchange for renumeration.

150. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and Members of the Class. Defendant also benefited from the receipt of Plaintiff's and Members of the Class's Personal Information, as this was required to facilitate the employment relationship and renumeration, as well as for the purpose of applying for employment.

151. As a result of Defendant's conduct, Plaintiff and Members of the Class suffered actual damages in an amount equal to the difference in value between the value of their labor with reasonable data privacy and security practices and procedures that Plaintiff and Members of the Classes were entitled to, and that labor without unreasonable data privacy and security practices and procedures that they received.

152. Under principals of equity and good conscience, Defendant should not be permitted to retain the monetary value of the labor belonging to Plaintiff and Members of the Classes because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself for which Plaintiff and Members of the Classes expended labor and that were otherwise mandated by federal, state, and local laws and industry standards.

153. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Members of the Class all unlawful or inequitable

proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, CHERYL COVINGTON, individually and on behalf of all others similarly situated, the Class as heretofore identified, respectfully prays for judgment as follows:

A. Certification for this matter to proceed as a class action on behalf of the proposed Class under Fed. R. Civ. Proc. 23;

B. Designation of Plaintiff as Class Representatives and designation of the undersigned as Class Counsel;

C. Actual damages in an amount according to proof;

D. Injunctive or declaratory relief;

E. Pre- and post-judgment interest at the maximum rate permitted by applicable law;

F. Costs and disbursements assessed by Plaintiff in connection with this action, including reasonable attorneys' fees pursuant to applicable law;

G. For attorneys' fees under the common fund doctrine and all other applicable law; and

H. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, hereby demands a trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable.

Dated: August 2, 2023

Respectfully submitted,

/s/ Joseph B. Alonso
Joseph B. Alonso
Georgia Bar No. 013627
ALONSO & WIRTH
1708 Peachtree Street
Suite 207
Atlanta, GA 30309
678-928-4472
Fax: 678-928-4472
jalonso@alonsowirth.com

Samuel Strauss*
Raina Borelli*
TURKE & STRAUSS, LLP
613 Williamson Street Suite 201
Madison, WI 53703
Ph: (608) 237-1775
Email: Sam@turkestrauss.com
Email: AustinD@turkestrauss.com

Lynn A. Toops*
Lisa M. La Fornara*
COHEN & MALAD, LLP
One Indiana Square
Suite 1400
Indianapolis, IN 46204
Tel: (317) 636-6481
ltoops@cohenandmalad.com
llafornara@cohenandmalad.com

J. Gerard Stranch, IV*
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC[52]
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com

* Admitted Pro Hac Vice
Counsel for Plaintiff and the Proposed Class

CERTIFICATE OF COMPLIANCE

Pursuant to Local Rule 7.1D, the attached pleading complies with the font and point selections prescribed by Local Rule 5.1B and uses 13 point Century Schoolbook Font.

/s/ Joseph B. Alonso
Joseph B. Alonso
Georgia Bar No. 013627

CERTIFICATE OF SERVICE

It is hereby certified that on August 2, 2023 this Amended Complaint was filed via the CM/ECF system, which will electronically serve all counsel of record.

/s/ Joseph B. Alonso
Joseph B. Alonso
Georgia Bar No. 013627

[52] Formerly Branstetter, Stranch & Jennings, PLLC

Exhibit A

Gifted Healthcare
Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

400597850000105600
000 0000135 00000000 0001 0002 00068 INS: 0 0
CHERYL COVINGTON
1410 WINDY RIDGE CT SE
CONYERS GA 30013-2986

August 24, 2022

Dear Cheryl Covington:

We are writing to inform you of a data security incident that may have involved your information as described below. We take the privacy and security of all information very seriously. While we have no evidence to suggest that any of the impacted information was misused during this incident, we are writing to inform you about the incident, our response, and steps you can take to help protect your information.

What Happened: We recently learned of suspicious activity related to an employee email account. Upon discovery, we took swift action to secure our email system and network. We also launched an internal investigation and engaged leading, independent cybersecurity specialists. Based on this investigation, we confirmed that three employee email accounts were subject to unauthorized access between August 25, 2021 and December 10, 2021. We then started a review of the entire mailbox contents in order to identify what information was impacted. On July 25, 2022, we completed this review, and we began working to review our internal files for up-to-date address information to provide individuals with notification.

What Information Was Involved: The types of information present within the affected mailboxes included your first and last name in combination with the following data elements: Account Number, Routing Number, Social Security Number.

What We Are Doing: Upon learning of this incident, we took the steps described above to address this incident. We have also implemented additional technical safeguards to enhance the security of information in our possession and prevent similar incidents from happening in the future. Additionally, we are offering you 12 months of complimentary credit monitoring and identity protection services. Due to privacy laws, we cannot register you directly. Additional information regarding how to enroll in the complimentary identity monitoring service is enclosed.

What You Can Do: We recommend that you remain vigilant in regularly reviewing and monitoring all of your accounts and explanation of benefits statements to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided the attached summary of steps you can take to help protect yourself against fraud and identity theft.

For More Information: We have established a dedicated assistance line to address any questions you may have which can be reached at 855-904-5625, Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays. You may also contact Gifted by mail at 3330 W Esplanade Ave Ste 505, Metairie, LA 70002. The security of our information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,

Gifted Healthcare Team

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Equifax® Credit Watch™ Gold provides you with the following key features:

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the Equifax website at **www.equifax.com/activate** and enter the Activation Code **304145896239** and follow the provided steps to receive your credit monitoring service online.
  - **Register:** Complete the form with your contact information and click "Continue".
    If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
  - **Create Account:** Enter your email address, create a password, and accept the terms of use.
  - **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
  - **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling.
- To sign up for US Mail delivery, dial **1-855-833-9162** for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only. You will be asked to enter your Activation Code home telephone number, home address, name, date of birth and Social Security Number. You will be asked to provide Equifax with your permission to access your Equifax credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment. Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

You can sign up for the online or offline credit monitoring service anytime between now and ***November 30, 2022***. Due to privacy laws, we cannot register you directly. Enrolling in this service will not affect your credit score. You must be over age 18 with a credit file to activate these services.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

---

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.