Kim D. Stephens, P.S., OSB #030635
Kaleigh N. Boyd (admitted *pro hac vice*)
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Telephone: 206-682-5600
Facsimile: 206-682-2992
kstephens@tousley.com
kboyd@tousley.com

Gary M. Klinger (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

Daniel O. Herrera (*pro hac vice* anticipated)
Nickolas J. Hagman (admitted *pro hac vice*)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Mason A. Barney (*pro hac vice* anticipated)
Tyler J. Bean (*pro hac vice* anticipated)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Attorneys for Plaintiffs and the Proposed Class

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
EUGENE DIVISION

In re: Kannact, Inc. Data Security Incident	Lead Case No. 6:23-cv-1132-AA

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Terry Dukes, Ann Fongheiser, and Alan White (collectively, "Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant Kannact, Inc. ("Kannact" or "Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from Kannact's failure to implement reasonable and industry standard data security practices.

2. Defendant is a digital health company that provides personal health coaching services to "identify fundamental gaps in care and provide people the support they need to close them."[1]

[1] https://kannact.com/ (last visited Aug. 30, 2023).

3. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

4. Kannact collected and maintained certain personally identifiable information of Plaintiffs and the putative Class Members (defined below), who are (or were) patients at Kannact and/or employees at companies that contracted with Kannact for services.

5. The Private Information compromised in the Data Breach included Plaintiffs' and Class Members' full names, email addresses, employee ID numbers, dates of birth, Social Security numbers, ("personally identifiable information" or "PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

6. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

7. As a result of the Data Breach, Plaintiffs and Class Members suffered concrete injuries in fact including, but not limited to: (i) Plaintiff Fongheiser's Private Information being disseminated on the dark web, according to IDX; (ii) experiencing an increase in spam calls, texts, and/or emails; (iii) Plaintiff Dukes experiencing two misuses of her Private Information via new accounts being opened (at Amazon and Roku) falsely under her name; (iv) invasion of privacy; (v) theft of their Private Information; (vi) lost or diminished value of Private Information; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs

associated with attempting to mitigate the actual consequences of the Data Breach; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' and the employees' in its network Private Information from a foreseeable and preventable cyber-attack.

8. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

9. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

10. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

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

14. Plaintiffs bring this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

15. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

16. Plaintiffs seek remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

17. Plaintiff Terry Dukes is a natural person and citizen of Tennessee.

18. Plaintiff Ann Fongheiser is a natural person and citizen of North Carolina.

19. Plaintiff Alan White is a natural person and citizen of Missouri.

20. Defendant Kannact, Inc. is a healthcare corporation organized under the laws of the State of Oregon with its principal place of business located at 425 2nd Avenue SW, Suite 201, Albany, Oregon 97321

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including each of Plaintiffs, is a citizen of a state different from Defendant.

22. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly conducts business in Oregon, and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

23. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant is a digital health company that provides personal health coaching services to "identify fundamental gaps in care and provide people the support they need to close them."[2]

25. Plaintiffs and Class Members are current and former patients at Defendant and/or current and former employees at companies that contracted with Defendant for services.

26. As a condition of receiving services at Defendant, Kannact requires that its customers entrust it with highly sensitive personal information.

27. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

28. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiffs and Class Members, that the Private Information collected from them as a condition of obtaining services at Kannact would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

29. Indeed, Defendant's Privacy Policy provides that: "[w]e employ technical, administrative and physical safeguards designed to protect your personal information. However,

[2] https://kannact.com/ (last visited Aug. 30, 2023).

no security measure can guarantee security and that data will not be accessed, disclosed, altered, or destroyed."[3]

30. Plaintiffs and Class Members provided their Private Information, directly or indirectly, to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

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

32. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep customer's Private Information safe and confidential.

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

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

[3] https://kannact.com/privacy (last visited Aug. 30, 2023).

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

The Data Breach

36. On or about August 23, 2023, Defendant began sending Plaintiffs and other Data Breach victims a Notice of Data Security Incident letter (the "Notice Letter"), informing them that:

> **What Happened?**
>
> On March 13, 2023, Kannact discovered that an unauthorized user had gained access to its system. Upon discovery of this Incident, Kannact promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. The preliminary findings determined that the cause of the unauthorized access was a third party file transfer software. While the forensics investigation was on going, Kannact provided substitute notice pursuant to HIPAA on April 12, 2023. Kannact engaged a third party data mining vendor to identify the covered entities involved, the specific individuals impacted, and the type of data that was in the file transfer software. On May 19, 2023, Kannact received a preliminary list of covered entities whose members were potentially impacted, however, data mining did not provide a full list of potentially impacted individuals or addresses for those they identify. On June 12, 2023, Kannact received another list of covered entities and impacted individuals, but without sufficient information to fully identify the individual or assign them to a covered entity. Kannact has been working to obtain addresses to provide sufficient notice to individuals. On June 13, 2023, the forensic investigation completed by the third party cybersecurity firm confirmed the cause of the unauthorized access to sensitive information was the third party file transfer software.
>
> **What Information Was Involved?**
>
> Based on the investigation, the following information related to you was subject to unauthorized access: Employee ID, Medications, Date of Birth, Name, Social Security, Email.

37. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members,

causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

38. The attacker accessed and acquired files Defendant shared with a third party containing the unencrypted Private Information of Plaintiffs and Class Members, including their Social Security numbers, PHI, and other sensitive information. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

39. As a result of the Data Breach, Plaintiff Fongheiser has been informed by IDX that her Private Information was disseminated on the dark web and Plaintiff Dukes has experienced attempts at opening fraudulent accounts in his name. Plaintiffs further believe that the Private Information of Plaintiffs Dukes, White, and Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

40. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

Data Breaches Are Preventable

41. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

42. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members,

causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

43. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, patients 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.
- 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.[4]

44. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

[4] *How to Protect Your Networks from Ransomware*, 3–4, *available at* https://www.justice.gov/criminal-ccips/file/872771/download.

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[5]

45. Given that Defendant was storing the Private Information of its current and former patients and/or clients' employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

46. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and, upon information and belief, the exposure of the Private Information of thousands of individuals, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, and Stores Plaintiffs' and the Class's Private Information

47. Defendant acquires, collects, and stores a massive amount of Private Information on its current and former patients as well as its clients' current and former employees.

48. As a condition of obtaining services from Kannact, Defendant requires that its patients and its clients' employees entrust it with highly sensitive personal information.

[5] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Sept. 5, 2023).

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

50. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

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

Defendant Knew or Should Have Known of the Risk Because Healthcare Entities In Possession Of Private Information Are Particularly Suspectable To Cyber Attacks

52. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the breach.

53. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

54. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[6]

55. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one

[6] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[7]

56. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

57. Defendant knew and understood unprotected or exposed Private Information in the custody of healthcare entities, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

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

---

[7] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360.com (Nov. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

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

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

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

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

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

64. As a healthcare entity in custody of its current and former patients' and its clients' current and former employees' Private Information, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiffs and Class

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

Value Of Personally Identifiable Information

65. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

66. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web.

67. Numerous sources cite dark web pricing for stolen identity credentials.[10] For example, PII can be sold at a price ranging from $40 to $200.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

---

[8] 17 C.F.R. § 248.201 (2013).
[9] *Id.*
[10] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Sept. 5, 2023).
[11] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Sept. 5, 2023).
[12] *In the Dark*, VPNOverview, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Sept. 5, 2023).

68. PII can sell for as much as $363 per record according to the Infosec Institute.[13] PII is particularly valuable because criminals can use it to target victims with frauds and scams.

69. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

70. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

71. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[14] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[15] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's

[13] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sept. 5, 2023).
[14] *Identity Theft and Your Social Security Number*, Social Security Administration (2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 5, 2023).
[15] *Id*.

employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

72. Moreover, it is not an easy task to change or cancel a stolen Social Security number:

> An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

73. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

74. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[17]

75. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

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

---

[16] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Sept. 5, 2023).

[17] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited Sept. 5, 2023).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

77. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[19]

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

Defendant Fails To Comply With FTC Guidelines

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

80. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines

[18] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited Sept. 5, 2023) ("GAO Report").
[19] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 5, 2023).

note that businesses should protect the personal patient 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.[20]

81. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21]

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

83. The FTC has brought enforcement actions against healthcare entities for failing to protect patient data adequately and reasonably, 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.

[20] *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 Sept. 5, 2023).
[21] *Id.*

84. These FTC enforcement actions include actions against healthcare entities like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (Kannact) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

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

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

87. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its patients and its clients' employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails To Comply With HIPAA Guidelines

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

89. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[22] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

[22] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

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

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

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

93. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

94. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

95. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is

required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

96. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

97. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[23]

98. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

99. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

[23] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

100. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[24] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[25]

Defendant Fails To Comply With Industry Standards

101. As noted above, experts studying cyber security routinely identify entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information that they collect and maintain.

102. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access

[24] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[25] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

103. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

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

105. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

106. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries

and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

The Data Breach Increases Victims' Risk Of Identity Theft

107. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

108. As Plaintiff Fongheiser has already experienced, the unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

109. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

110. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take

on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

111. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

112. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[26]

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

[26] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited Sept. 5, 2023).

114. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

115. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

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

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

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

118. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

119. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice Letter instructs,[27] "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

120. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, researching the credit monitoring and identity theft protection services offered by Defendant, and reviewing their credit reports and financial account statements for any indication of fraudulent activity, which may take years to detect.

121. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

122. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[29]

123. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data

[27] Notice Letter.
[28] *See* GAO Report, *supra* n.19.
[29] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Sept. 5, 2023).

breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[30]

Diminution Value Of Private Information

124. PII and PHI are valuable property rights.[31] Their value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

125. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[32]

126. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[33,34]

127. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[35]

128. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[36]

---

[30] *See* GAO Report, *supra* n.19 at 2.

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

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

[33] https://datacoup.com/

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

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

[36] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),

129. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

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

131. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

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

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

---

https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sept. 5, 2023).

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

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

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

136. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, the volume of data obtained in the Data Breach, and Plaintiff Fongheiser's Private Information already being disseminated on the dark web (according to IDX), there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

137. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

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

139. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss Of The Benefit Of The Bargain

140. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for the provision of medical services and/or providing labor to Defendant's clients, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information and/or obtaining an employment position with adequate data security, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services and/or employment positions that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant and/or its clients.

PLAINTIFFS' EXPERIENCES

Plaintiff Terry Dukes

141. Plaintiff Dukes received a notice from Defendant that her PII and PHI had been improperly accessed and/or obtained by third parties.

142. Plaintiff Dukes would not have entrusted her Private Information to Defendant had she been aware of Defendant's inadequate data security policies and procedures.

143. The notice indicated that Plaintiff Dukes' PII, inclusive of her full name, date of birth, address, phone number, Social Security number, driver's license number, and her protected

health information, including but not limited to her medical diagnosis, treatment, and pharmaceutical records and her Kannact ID, were compromised in the Data Breach.

144. As a result of the Data Breach, Plaintiff Dukes has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services. Plaintiff Dukes has spent several hours dealing with the Data Breach, valuable time Plaintiff Dukes otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

145. Following Plaintiff Dukes' receipt of Defendant's notice of the Data Breach, Plaintiff Dukes has received two notices regarding misuse of her Private Information, alerting her that new accounts have been opened in her name with Amazon and Roku.

146. Plaintiff Dukes also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which upon information and belief, was caused by the Data Breach

147. As a result of the Data Breach, Plaintiff Dukes has suffered anxiety as a result of the release of her Private Information, which she believed Defendant would protect from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Dukes is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

148. Plaintiff Dukes suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and

diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Dukes; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

149. As a result of the Data Breach, Plaintiff Dukes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

150. As a result of the Data Breach, Plaintiff Dukes is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Ann Fongheiser

151. Plaintiff Ann Fongheiser is a current employee at Pathways, which, upon information and belief, contracted with Defendant for services.

152. Plaintiff Fongheiser would not have entrusted her Private Information to Defendant had she been aware of Defendant's inadequate data security policies and procedures.

153. As a condition of her employment at Pathways, she was required to provide her Private Information, indirectly or directly, to Defendant.

154. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Fongheiser's Private Information in its system.

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

156. Plaintiff Ann Fongheiser received the Notice Letter, by U.S. mail, directly from Defendant, dated August 23, 2023. According to the Notice Letter, Plaintiff Fongheiser's PII and PHI was improperly accessed and obtained by unauthorized third parties, including her name, email address, employee ID, Social Security number, date of birth, and medications.

157. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Fongheiser made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter as well as checking their financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Fongheiser has spent significant time dealing with the Data Breach, valuable time Plaintiff Fongheiser otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

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

159. Plaintiff Fongheiser further suffered actual injury in the form of her Private Information being disseminated on the dark web, according to IDX, which upon information and belief, was caused by the Data Breach.

160. Plaintiff Fongheiser also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which upon information and belief, was caused by the Data Breach.

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

162. As a result of the Data Breach, Plaintiff Fongheiser anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

163. As a result of the Data Breach, Plaintiff Fongheiser is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

Plaintiff Alan White

165. Plaintiff White entrusted his Private Information to Defendant through his employment with one of Defendant's clients, Pathways a/k/a Camelot Cares.

166. Plaintiff White would not have entrusted his Private Information to Defendant had he been aware of Defendant's inadequate data security policies and procedures.

167. Plaintiff White's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

168. As a direct and proximate result of Kannact's actions and omissions, Plaintiff White has been harmed and is at an imminent, immediate, and continuing increased risk of harm, especially given the fraudulent misuse of Plaintiff Duke's Private Information that has already taken place, and the fact that Plaintiff Fongheiser's Private Information has been discovered on the dark web.

169. Further, as a direct and proximate result of Kannact's conduct, Plaintiff White has been forced to spend time dealing with the effects of the Data Breach.

170. Plaintiff White also faces a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of his Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against him.

171. Additionally, Plaintiff White has spent and will continue to spend significant amounts of time monitoring his accounts and records for misuse.

172. Finally, Plaintiff White has suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of his time reasonably incurred to remedy or mitigate the effects of the Data Breach.

173. Moreover, Plaintiff White has an interest in ensuring that his Private Information, which is believed to still be in the possession of Kannact, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

174. As a direct and proximate result of Kannact's actions and inactions, Plaintiff White has suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

CLASS ACTION ALLEGATIONS

175. This action is properly maintainable as a class action. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated.

176. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **Nationwide Class**
> All individuals residing in the United States whose Private Information was compromised in the data breach announced by Defendant in August 2023 (the "Class").

177. In addition, Plaintiff Dukes proposes the following Tennessee Subclass definition, subject to amendment as appropriate:

> **Tennessee Subclass**
> All individuals residing in the State of Tennessee whose Private Information was compromised in the data breach announced by Defendant in August 2023 (the "Tennessee Subclass").

178. Plaintiff Fongheiser proposes the following North Carolina Subclass definition, subject to amendment as appropriate:

> **North Carolina Subclass**
> All individuals residing in the State of North Carolina whose Private Information was compromised in the data breach announced by Defendant in August 2023 (the "North Carolina Subclass").

179. Plaintiff White proposes the following Missouri Subclass definition, subject to amendment as appropriate:

> **Missouri Subclass**
> All individuals residing in the State of Missouri whose Private Information was compromised in the data breach announced by Defendant in August 2023 (the "Missouri Subclass").

180. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

181. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of Class Members is currently unknown to Plaintiffs and exclusively in Defendant's possession, upon information and belief, thousands of Class Members were impacted in the Data Breach. The Classes are apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

182. Common questions of law and fact exist as to all members of the Class that predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class, which may affect individual Class members, include, but are not limited to, the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g.. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. 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;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and

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

183. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

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

Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

185. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

186. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

187. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources;

the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

188. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

189. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

190. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

191. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Code of Civil Procedure § 382.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

192. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

193. Defendant requires its patients and its clients' employees, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its medical services.

194. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its patients and its clients' employees, which solicitations and services affect commerce.

195. Plaintiffs and Class Members entrusted Defendant with their Private Information, directly or indirectly, with the understanding that Defendant would safeguard their information.

196. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

197. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

198. 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.

199. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

200. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not notify Plaintiffs or some Class Members of the Data Breach until August 23, 2023, despite Defendant knowing on or about March 13, 2023 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiffs and the Class.

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

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

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

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

205. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information it was no longer required to retain pursuant to regulations.

206. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

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

208. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

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

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

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

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

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

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

209. Defendant violated Section 5 of the FTC Act and HPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

210. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

211. Plaintiffs and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

212. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

213. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

214. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

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

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

217. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

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

219. 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.

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

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

222. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

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

224. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

226. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) Plaintiff Fongheiser's Private Information being disseminated on the dark web, according to IDX; (ii) Plaintiff Dukes experiencing two misuses of her Private Information via new accounts being opened (at Amazon and Roku) falsely under her name; (iii) experiencing an increase in spam calls, texts, and/or

emails; (iv) invasion of privacy; (v) theft of their Private Information; (vi) lost or diminished value of Private Information; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' and the employees' in its network Private Information from a foreseeable and preventable cyber-attack.

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

228. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

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

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

231. Plaintiffs 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 Plaintiffs and the Class)

232. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

233. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair... practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

234. Defendant's duty to use reasonable security measures also arose under the HIPAA, under which it was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

235. Defendant owed a duty of care in protecting Plaintiffs' and Class Members' Private Information, pursuant to Section 5 of the FTC Act, HIPAA, and an independent duty of care.

236. Defendant violated Section 5 of the FTC Act, HIPAA, and similar state statutes by failing to use reasonable measures to protect Private Information and not complying with

industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

237. In its Privacy Policy, Defendant promises its customers that it will not disclose customers' Private Information, outside of the excepted circumstances set forth therein–none of which apply here. However, Plaintiffs' and Class Members' Private Information has been disclosed without their written authorization as a result of the Data Breach.

238. As evidenced by the occurrence of the Data Breach, Defendant negligently misrepresented its data security measures and Privacy Policy to Plaintiffs and Class Members.

239. Defendant violated Section 5 of the FTC Act and HIPAA by negligently misrepresenting its data security practices to Plaintiffs and Class Members.

240. Defendant violated Section 5 of the FTC Act and HIPAA by breaching its duties of care to Plaintiffs and Class Members, as provided in its Privacy Policy.

241. Defendant further violated Section 5 of the FTC Act and HIPAA by failing to ensure that its vendors use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and shared and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

242. Defendant's violation of Section 5 of the FTC Act, HIPAA, and other duties (listed above) constitutes negligence *per se.*

243. Class members are customers within the class of persons that Section 5 of the FTC Act, HIPAA, and similar state statutes intended to protect.

244. Moreover, the harm that has occurred is the type of harm that the FTC Act, HIPAA, and similar state statutes were intended to guard against. Indeed, the FTC has pursued over numerous enforcement actions against insurance companies which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

245. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

247. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) Plaintiff Fongheiser's Private Information being disseminated on the dark web, according to IDX; (ii) Plaintiff Dukes experiencing two misuses of her Private Information via new accounts being opened (at Amazon and Roku) falsely under her name; (iii) experiencing an increase in spam calls, texts, and/or emails invasion of privacy; (iv) theft of their Private Information; (v) lost or diminished value of Private Information; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual

consequences of the Data Breach; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' and the employees' in its network Private Information from a foreseeable and preventable cyber-attack.

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

249. As a direct and proximate result of Defendant's negligence *per se*, the products and/or services that Defendant provided to Plaintiffs and Class Members damaged other property, including the value of their Private Information.

250. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

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

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

253. Plaintiffs 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 III
Breach Of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and the Class)

254. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

255. Upon information and belief, Kannact entered into virtually identical contracts with its clients, including Plaintiffs' employers, to provide healthcare services to them, which included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

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

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

258. Defendant breached its contracts with its clients and, as a result, Plaintiffs and Class Members were affected by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

259. As foreseen, Plaintiffs and the Class were harmed by Defendant' failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

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

COUNT IV
Bailment
(On Behalf of Plaintiffs and the Class)

261. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

262. Plaintiffs' and Class members' Private Information was provided to Defendant.

263. In delivering their Private Information, Plaintiffs and Class members intended and understood that their Private Information would be adequately safeguarded and protected.

264. Defendant accepted Plaintiffs' and Class members' Private Information.

265. By accepting possession of Plaintiffs' and Class members' Private Information, Defendant understood that Plaintiffs and the Class expected their Private Information to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

266. During the bailment (or deposit), Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care, diligence, and prudence in protecting their Private Information.

267. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class members' Private Information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class members' Private Information.

268. Defendant further breached its duty to safeguard Plaintiffs' and Class members' Private Information by failing to timely notify them that their Private Information had been compromised as a result of the Data Breach.

269. Defendant failed to return, purge, or delete the Private Information belonging to Plaintiffs and Class members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

270. As a direct and proximate result of Defendant's breach of its duties, Plaintiffs and the Class suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth herein.

271. As a direct and proximate result of Defendant's breach of its duty, Plaintiffs' and Class members Private Information that was entrusted to Defendant during the bailment (or deposit) was damaged and its value diminished.

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

272. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

273. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from and/or provided their labor to Defendant as well as provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services and/or employment position that were the

subject of the transaction and should have had their Private Information protected with adequate data security.

274. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

275. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

276. Defendant acquired the Private Information through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

277. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information at Defendant or obtained services at Defendant.

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

279. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

280. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) Plaintiff Fongheiser's Private Information being disseminated on the dark web, according to IDX; (ii) Plaintiff Dukes experiencing two misuses of her Private Information via new accounts being opened (at Amazon and Roku) falsely under her name; (iii) experiencing an increase in spam

calls, texts, and/or emails invasion of privacy; (iv) theft of their Private Information; (v) lost or diminished value of Private Information; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' and the employees' in its network Private Information from a foreseeable and preventable cyber-attack.

281. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

282. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
Violations of Oregon Unlawful Trade Practices Act
(On Behalf of Plaintiffs and the Class)

283. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

284. Plaintiffs are authorized to bring this claim under Or. Rev. Stat. § 646.638(1).

285. Or. Rev. Stat. § 646.608(1), *et seq*. ("OUTPA"), prohibits "unlawful practice[]s in the course of the person's business, vocation or occupation...." Or. Rev. Stat. § 646.608(1).

286. As described in this Complaint, Defendant has engaged in the following unfair or deceptive acts or practices in violation of the OUTPA:

(e) Represent[ing] that real estate, goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, quantities or qualities that the real estate, goods, or services do not have or that a person has a sponsorship, approval, status, qualification, affiliation, or connection that the person does not have;

(g) Represent[ing] that real estate, goods or services are of a particular standard, quality, or grade, or that real estate or goods are of a particular style or model, if the real estate, goods or services are of another; and

(u) Engag[ing] in any other unfair or deceptive conduct in trade or commerce.

Or. Rev. Stat. §§ 646.608(e), (g), (u).

287. Defendant's deceptive acts or practices in the conduct of commerce include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including but not limited to duties imposed by the FTC Act and HIPAA, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information; and

h. Failing to promptly and adequately notify Plaintiffs and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

288. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant's relevant acts, practices, and omissions complained of in this action were done in the

course of Defendant's business of marketing, offering for sale, and selling goods and services to consumers throughout the United States.

289. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiffs' and Class members' Private Information. This exclusive knowledge includes, but is not limited to, information that Defendant received through internal and other non-public audits and reviews that concluded that Defendant's security policies were substandard and deficient, and that Plaintiffs' and Class members' Private Information and other Defendant data was vulnerable.

290. Defendant had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

291. Defendant also had exclusive knowledge about the length of time that it maintained individuals' Private Information after they stopped using services that necessitated the transfer of that Private Information to Defendant.

292. Defendant failed to disclose, and actively concealed, the material information it had regarding Defendant's deficient security policies and practices and regarding the security of the sensitive Private Information. For example, even though Defendant has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiffs' and Class members' Private Information was vulnerable as a result, Defendant failed to disclose this information to, and actively concealed this information from, Plaintiffs, Class members and the public. Defendant also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former patients' Private Information and other records.

293. Likewise, during the days and weeks following the Data Breach, Defendant failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

294. Defendant had a duty to disclose the material information that it had because, inter alia, it had exclusive knowledge of the information, it actively concealed the information, and because Defendant was in a fiduciary position by virtue of the fact that Defendant collected and maintained Plaintiffs' and Class members' Private Information.

295. Defendant's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and its ability to protect the confidentiality of current and former patients' and/or employees' Private Information.

296. Had Defendant disclosed to Plaintiffs and the Class that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Class members' Private Information without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their Private Information.

297. Accordingly, Plaintiffs and Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

298. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws such as HIPAA and the FTC Act.

299. The injuries suffered by Plaintiffs and the Class greatly outweigh any potential countervailing benefit to consumers or to competition and are not injuries that Plaintiffs and the Class should have reasonably avoided.

300. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and the Class as a direct result of Defendant's deceptive acts and practices as set forth herein include, without limitation: (i) Plaintiff Fongheiser's Private Information being disseminated on the dark web, according to IDX; (ii) Plaintiff Dukes experiencing two misuses of her Private Information via new accounts being opened (at Amazon and Roku) falsely under her name; (iii) experiencing an increase in spam calls, texts, and/or emails; (iv) invasion of privacy; (v) theft of their Private Information; (vi) lost or diminished value of Private Information; (vii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (viii) loss of benefit of the bargain; (ix) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' and the employees' in its network Private Information from a foreseeable and preventable cyber-attack.

301. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction

barring Defendant from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VII
Violations of Tennessee Consumer Protection Act
(On Behalf of Plaintiff Dukes and the Tennessee Subclass)

302. Plaintiff Dukes ("Plaintiff" for the purposes of this count) restates and realleges the preceding factual allegations set forth above, as if fully alleged herein, and brings this claim on behalf of herself and the Tennessee Subclass (the "Class" for the purposes of this count).

303. Plaintiff is authorized to bring this claim under Tenn. Code Ann. § 47-19-109(a).

304. Tenn. Code Ann. § 47-18-104, et seq. ("TCPA"), prohibits "unfair or deceptive acts or practices affecting the conduct of any trade or commerce . . . ." Tenn. Code Ann. § 47-18-104(a).

305. As described in this Complaint, Defendant has engaged in the following unfair or deceptive acts or practices in violation of the TCPA:

(5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or qualities that they do not have or that a person has a sponsorship approval, status, affiliation or connection that such person does not have; and

(7) Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another.

Tenn. Code Ann. §§ 47-18-104(b)(5), (7).

306. Defendant's deceptive acts or practices in the conduct of commerce include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information; and

h. Failing to promptly and adequately notify Plaintiff and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

307. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant's relevant acts, practices, and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services to consumers throughout the United States.

308. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiff's and Class members' Private Information. This exclusive knowledge includes, but is not limited to, information that Defendant received through internal and other non-public audits and reviews that concluded that Defendant's security policies were substandard and deficient, and that Plaintiff's and Class members' Private Information and other Defendant data was vulnerable.

309. Defendant had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

310. Defendant also had exclusive knowledge about the length of time that it maintained individuals' Private Information after they stopped using services that necessitated the transfer of that Private Information to Defendant.

311. Defendant failed to disclose, and actively concealed, the material information it had regarding Defendant's deficient security policies and practices, and regarding the security of the sensitive Private Information. For example, even though Defendant has long known through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiff's and Class members' Private Information was vulnerable as a result, Defendant failed to disclose this information to, and actively concealed this information from,

Plaintiff, Class members and the public. Defendant also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former patients' Private Information and other records. Likewise, during the days and weeks following the Data Breach, Defendant failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

312. Defendant had a duty to disclose the material information that it had because, inter alia, it had exclusive knowledge of the information, it actively concealed the information, and because Defendant was in a fiduciary position by virtue of the fact that Defendant collected and maintained Plaintiff's and Class members' Private Information.

313. Defendant's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and its ability to protect the confidentiality of current and former patients' and/or employees' Private Information.

314. Had Defendant disclosed to Plaintiff and the Class that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class members' Private Information without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their Private Information.

315. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

316. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as HIPAA and the FTC Act.

317. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition and are not injuries that Plaintiff and the Class should have reasonably avoided.

318. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct result of Defendant's deceptive acts and practices as set forth herein include the following:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their Private Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised

accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

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

g. damages to and diminution in value of their personal information entrusted to Defendant, and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the data in its possession.

319. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper

COUNT VIII
Violations of the Tennessee Data Breach Notification Statute
(On Behalf of Plaintiff Dukes and the Tennessee Subclass)

320. Plaintiff Dukes ("Plaintiff" for the purposes of this count) restates and realleges the preceding factual allegations set forth above, as if fully alleged herein, and brings this claim on behalf of herself and the Tennessee Subclass (the "Class" for the purposes of this count).

321. Plaintiff is authorized to bring this claim under Tenn. Code Ann. § 47-18-2107(h).

322. Defendant is a corporation that owns, maintains, and records Private Information, and computerized data including Private Information, about its current and former patients and/or employees, including Plaintiff and Class members.

323. Defendant is in possession of Private Information belonging to Plaintiff and Class members and is responsible for reasonably safeguarding that Private Information consistent with the requirements of Tenn. Code Ann. § 47-18-2107. 2

324. Defendant failed to safeguard, maintain, and dispose of, as required, the Private Information within its possession, custody, or control as discussed herein, which it was required to do by Tennessee law.

325. Defendant, knowing and/or reasonably believing that Plaintiff's and Class members' Private Information was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members, as required by Tenn. Code Ann. § 47-18-2107(b).

326. As a result of Defendant's failure to reasonably safeguard Plaintiff's and Class members' Private Information, and the failure to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their Private Information in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

COUNT IX
Violations of the North Carolina Identity Theft Protection Act
(On Behalf of Plaintiff Fongheiser and the North Carolina Subclass)

327. Plaintiff Fongheiser ("Plaintiff" for the purposes of this count) restates and realleges the preceding factual allegations set forth above, as if fully alleged herein, and brings this

claim on behalf of herself and the North Carolina Subclass (the "Class" for the purposes of this count).

328. Kannact is a business that owns or licenses computerized data that includes Plaintiff's and Class Members' sensitive personal and medical information (for the purpose of this count, "Private Information"), as defined by N.C. Gen. Stat. § 75- 61(1).

329. Plaintiff and North Carolina Subclass Members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

330. Kannact is required to accurately notify Plaintiff and North Carolina Subclass Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

331. Plaintiff's and North Carolina Subclass Members' Private Information includes information as covered under N.C. Gen. Stat. § 75-61(10).

332. Because Kannact discovered a security breach and had notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), Kannact had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

333. By failing to disclose the Data Breach in a timely and accurate manner, Kannact violated N.C. Gen. Stat. § 75-65.

334. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

335. As a direct and proximate result of Kannact's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass Members suffered damages, including but not limited to Plaintiff's Private Information being disseminated onto the dark web, as alleged herein.

336. Plaintiff and North Carolina Subclass Members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorneys' fees.

COUNT X
Violations of the Missouri Merchandise Practices Act
(On Behalf of Plaintiff White and the Missouri Subclass)

337. Plaintiff White ("Plaintiff" for the purposes of this count) restates and realleges the preceding factual allegations set forth above, as if fully alleged herein, and brings this claim on behalf of himself and the Missouri Subclass (the "Class" for the purposes of this count).

338. Kannact is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

339. Kannact engaged in "sales" of and "advertisements" for "merchandise" in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, including Plaintiff and the Missouri Subclass, as defined by Mo. Rev. Stat. § 407.010(1), (4), (6) and (7).

340. Kannact engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Missouri Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and properly improve security and privacy measures despite knowing the risk

of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Missouri Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff and Missouri Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Missouri Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

341. Kannact's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Kannact's data security and ability to protect the confidentiality of consumers' Private Information.

342. Kannact intended to mislead Plaintiff and Missouri Subclass Members and induce them to rely on its misrepresentations and omissions.

343. Kannact acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass Members' rights.

344. As a direct and proximate result of Kannact's unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Kannact's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

345. Plaintiff, on behalf of Missouri Subclass Members, seeks all monetary and nonmonetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

COUNT XI
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

346. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

347. 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 to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described herein.

348. 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 Plaintiffs' and Class members' Private Information, and whether Defendant are currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information. Plaintiffs alleges that Defendant's data security measures remain inadequate.

349. Plaintiffs and the Class continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

350. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant continues to owe a legal duty to secure Plaintiffs' and Class members' Private Information, to timely notify them of any data breach, and to establish and implement data security measures that are adequate to secure Private Information.

351. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect Plaintiffs' and Class members' Private Information.

352. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury, and they lack an adequate legal remedy to address their harms. The threat of another breach of the Private Information in Defendant's possession, custody, and control is real, immediate, and

substantial. If another breach of Defendant's network, systems, servers, or workstations occurs, Plaintiffs and the Class will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

353. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at Defendant, Plaintiffs and the Class will likely be subjected to substantial identity theft and other damage. 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.

354. Issuance of the requested injunction will serve the public interest by preventing another data breach at Defendant, thus eliminating additional injuries to Plaintiffs and the thousands of Class members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class and Subclasses;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs 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 injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

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

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

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

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

v. Prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to

conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

x. Requiring Defendant to conduct regular database scanning and securing checks;

xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security

personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

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

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

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

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

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

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

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

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

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

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

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

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: October 25, 2023

Respectfully submitted,

s/ Kim D. Stephens
Kim D. Stephens, P.S., OSB #030635
s/ Kaleigh N. Boyd
Kaleigh N. Boyd (admitted *pro hac vice*)
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Telephone: 206-682-5600
Facsimile: 206-682-2992
kstephens@tousley.com
kboyd@tousley.com

Gary M. Klinger (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

Daniel O. Herrera (*pro hac vice* anticipated)
Nickolas J. Hagman (admitted *pro hac vice*)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Mason A. Barney (*pro hac vice* anticipated)
Tyler J. Bean (*pro hac vice* anticipated)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Attorneys for Plaintiffs and the Proposed Class