UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

ALEXIS SANCHEZ, on behalf of himself and all others similarly situated,

Plaintiff,

v.

CAVENDER STORES, LTD.,

Defendant.

Case No.: 4:22-CV-01016

COMPLAINT—CLASS ACTION

DEMAND FOR JURY TRIAL

Alexis Sanchez ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Cavender Stores, Ltd. ("Cavender's" and "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a Western clothing retail store with locations throughout the South and Southwest. Today, Defendant boasts 94 stores—ranging from Las Vegas, Nevada, to Orlando, Florida.[1]

[1] *Store Locator*, CAVENDER'S, https://www.cavenders.com/storelocator/ (last accessed Nov. 19, 2022).

3. As a major employer, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "Private Information." But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in an April 2022 data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to consumer Private Information.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's Private Information. In short, Defendant's failures placed the Class's Private Information in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, receiving a breach notice dated July 20, 2022. He brings this class action on behalf of himself, and all others harmed by Defendant's misconduct.

PARTIES

7. Plaintiff, Alexis Sanchez, is natural person and citizen of Texas. He resides at 901 Roaming Road Drive, in Allen, Collin County Texas in the Eastern District of Texas where he intends to remain.

8. Defendant, Cavender Stores, Ltd., is a domestic limited partnership which is headquartered in the Eastern District of Texas.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are over 100 putative Class Members. And minimal diversity is established because while Defendant is based in Texas, it employed—and continues to employ—natural persons in, *inter alia*, Alabama, Arkansas, Colorado, Florida, Georgia, Kansas, Louisiana, Mississippi, Missouri, Nebraska, Nevada, New Mexico, Oklahoma, and Tennessee, all of whom are members of the putative class.

10. This Court has personal jurisdiction over Defendant because it is headquartered in the Eastern District of Texas, regularly conducts business in Texas, and has sufficient minimum contacts in Texas.

11. Venue is proper in this Court under 28 U.S.C. § 1391(b)(2) because Defendant's headquarters are in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the Private Information of Plaintiff and the Class

12. Defendant is a Western clothing retail store with locations throughout the South and Southwest.

13. As part of its business, Defendant receives and maintains the Private Information of thousands of individuals. In doing so, Defendant agrees to safeguard their Private Information. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Private

Information. After all, Defendant declares that it "understands that you care about the privacy of your information."[2]

14. And under state and federal law, businesses like Defendant have duties to protect consumers' Private Information and to notify them about breaches.

15. Defendant recognizes these duties, declaring that "[w]e value the trust you place in us to protect your privacy and take our responsibility to safeguard your personal information seriously."[3]

16. Defendant advertises that "[w]e do not use or release any credit card or personal information for any purpose other than the purpose for which you provide it."[4] More broadly, Defendant proclaims that "we will not use or share your information."[5]

Defendant's Data Breach

17. Defendant failed its duties when its inadequate security practices caused the Data Breach.

18. On April 27, 2022, Defendant was hacked.[6] The Data Breach appeared to last for two days, as Defendant reported that the "end of the breach" was on April 29, 2022.[7]

19. Because of Defendant's Data Breach, the following types of Private Information were compromised: names, addresses, Social Security numbers, financial account numbers, credit card numbers, debit card numbers, medical information, health insurance information, and the names of employees' children.[8]

---

[2] *Privacy Policy*, CAVENDER'S https://www.cavenders.com/privacy-policy.html (last accessed Nov. 19, 2022).
[3] *Notice of Data Breach*, CAVENDER'S (July 20, 2022) https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-414.pdf.
[4] *Privacy Policy*, CAVENDER'S https://www.cavenders.com/privacy-policy.html (last accessed Nov. 19, 2022).
[5] *Id*.
[6] *Reported Data Breach Incidents*, ATTORNEY GEN. MONTANA, https://dojmt.gov/consumer/databreach/ (last accessed Nov. 19, 2022).
[7] *Id*.
[8] *Data Security Breach Reports*, ATTORNEY GEN. TEXAS,

20. This exposure of children's Private Information is particularly egregious. In its Notice of Data Breach, Defendant declares that "Cavender Stores, Ltd. ("Cavender's") values and respects the privacy of your child's information."[9] But Defendant admits that the Data Breach exposed "some of your child's personal information" and "could include your child's name."[10] And so, Defendant warned parents and guardians to "protect your child from the misuse of his or her information."[11]

21. By mid-May 2022, Defendant realized that files were, in fact, stolen. Specifically, Defendant discovered that its "employee benefits and payroll files were copied from our system."[12]

22. In total, Defendant injured tens of thousands of individuals (the "Class")—via the exposure of their Private Information—in the Data Breach. In Texas alone, 21,145 individuals were exposed.[13] Upon information and belief, these tens of thousands of people include Defendant's current employees, former employees—and the children of Defendant's current and former employees.

23. Since the breach, Defendant has "implemented remediation activities, and . . . taken steps to help prevent a similar incident from happening."[14] But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

---

https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last accessed Nov. 19, 2022).
[9] *Id*.
[10] *Id*.
[11] *Id*.
[12] *Notice of Data Breach*, CAVENDER'S (July 20, 2022) https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-414.pdf.
[13] *Data Security Breach Reports*, ATTORNEY GEN. TEXAS, https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last accessed Nov. 19, 2022).
[14] *Notice of Data Breach*, CAVENDER'S (July 20, 2022) https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-414.pdf.

24. Then, Defendant impermissibly delayed notifying the victims of the Data Breach. After all, it took Defendant nearly *three months* to begin notifying the victims. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner. By delaying the notification process, Defendant allowed the injuries of Plaintiff and the Class to fester and spread.

25. Not only did Defendant expose the Class to cybercriminals, but Defendant exposed the Class to a malicious and effective ransomware group. Several entities reported that the Data Breach was conducted by the cybercriminal group "Black Basta."[15] And one website reports that "100%" of the stolen files were leaked.[16] That same website reports that the "number of times victim post has been viewed" is already at 739 times.[17]

26. Black Basta is a particularly notorious ransomware group.[18] Described as a "formidable threat" who are "likely seasoned cybercriminals," Black Basta hacked twenty-two organization in June 2022 *alone*.[19] For example, the American Dental Association was hacked by Black Basta—who then proceeded to leak the stolen data is just ninety-six hours.[20]

27. This information underscores the severity of injuries that Plaintiff and Class Members suffered.

28. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures. And Defendant's

[15] *Cavenders*, BREACHSENSE https://www.breachsense.io/breaches/cavenders/ (last accessed Nov. 19, 2022); *Black Basta Ransomware Victim: CAVENDERS*, REDPACKET Security (June 7, 2022) https://www.redpacketsecurity.com/black-basta-ransomware-victim-cavenders/.
[16] REDPACKET Security (June 7, 2022) https://www.redpacketsecurity.com/black-basta-ransomware-victim-cavenders/.
[17] *Id*.
[18] *Black Basta*, TRENDMICRO (Sept. 1, 2022) https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta; *Black Basta ransomware – what you need to know*, TRIPWIRE (June 30, 2022) https://www.tripwire.com/state-of-security/black-basta-ransomware-what-you-need-to-know.
[19] *Id*.
[20] *Id*.

negligence is further evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Private Information.

29. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and other services. But upon information and belief, these conciliatory services are wholly insufficient to compensate Plaintiff and Class Members for the injuries that Defendant inflicted upon them.

30. In sum, because of Defendant's Data Breach, the sensitive Private Information of Plaintiff and Class Members was placed into the hands of sophisticated cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

Plaintiff's Experiences and Injuries

31. Plaintiff Alexis Sanchez was injured by Defendant's Data Breach. Plaintiff was employed by Defendant from 2015–2017 as a cashier and salesman.

32. To Plaintiff's knowledge, his sensitive information has never been compromised by a data breach. But Defendant's Data Breach changed that.

33. Plaintiff received a Notice of Data Breach dated July 20, 2022. Then, in October 2022, Plaintiff spoke with a store manager and confirmed that he was exposed in the Data Breach.

34. Through its Data Breach, Defendant compromised Plaintiff's name, birth date, Social Security number, and banking information.

35. Plaintiff hoped to sign up for the protection services that Defendant offered. But on information and belief, Plaintiff was unable to as the services had expired.

36. Since the exposure of his Private Information, Plaintiff has begun receiving spam texts and or phone calls.

37. But far worse, Plaintiff has suffered significant fraud and identify theft. Specifically:

a. The Internal Revenue Service (IRS) sent Plaintiff a letter declaring that a business was started in his name; and

b. The United States Postal Service (USPS) notified Plaintiff that someone attempted to change his official address.

38. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

39. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

40. Plaintiff suffered actual injury from the exposure (and likely theft) of his Private Information—which violates his rights to privacy.

41. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

42. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

43. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

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

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

45. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

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

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. Lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of their stolen Private Information; and

h. The continued risk to their Private Information—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

46. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained.

47. The value of Plaintiff and Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

48. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the Private Information far and wide.

49. One way that criminals profit from stolen Private Information is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen Private Information, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

50. The development of "Fullz" packages means that the Private Information exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

51. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can 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. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact,

including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

52. Defendant disclosed the Private Information of Plaintiff and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiff and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

53. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

54. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and or data breaches in recent years.

55. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[21]

56. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have

[21] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

lesser IT defenses and a high incentive to regain access to their data quickly."[22]

57. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

58. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

59. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[23] The FTC declared that, *inter alia*, businesses must:

a. Protect the personal customer information that they keep;

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

c. Encrypt information stored on computer networks;

d. Understand their network's vulnerabilities; and

e. Implement policies to correct security problems.

60. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

61. Furthermore, the FTC explains that companies must:

a. Not maintain information longer than is needed to authorize a transaction;

b. Limit access to sensitive data;

[22] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[23] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

c. Require complex passwords to be used on networks;

d. Use industry-tested methods for security;

e. Monitor for suspicious activity on the network; and

f. Verify that third-party service providers use reasonable security measures.

62. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use 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.

63. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to consumers' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

64. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

65. Other industry standard best practices 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; and training staff regarding critical points.

66. 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.

67. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

68. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep people's medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[24]

69. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information is properly maintained.[25]

[24] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[25] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

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

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

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

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

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

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

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

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security

incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

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

71. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

72. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose Private Information was compromised in the Data Breach discovered by Cavender Stores, Ltd. in April 2022, including all those who received notice of the Data Breach.

73. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

74. Plaintiff reserves the right to amend the class definition.

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

76. **Ascertainability**. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

77. **Numerosity**. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least NUMBER members.

78. **Commonality and Predominance**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. If Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Private Information;

b. If Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Defendant were negligent in maintaining, protecting, and securing Private Information;

d. If Defendant breached contract promises to safeguard Plaintiff's and the Class's Private Information;

e. If Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. If Defendant's Breach Notice was reasonable;

g. If the Data Breach caused Plaintiff's and the Class's injuries;

h. What the proper damages measure is; and

i. If Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

79. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's common interests. his interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

80. **Superiority.** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

81. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

82. Plaintiff and Class Members entrusted their Private Information to Defendant.

83. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Private Information in a data breach. And here, that foreseeable danger came to pass.

84. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and Class Members' Private Information by:

a. Disclosing and providing access to this information to third parties; and

b. Failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

85. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class Members' Private Information.

86. Defendant owed—to Plaintiff and Class Members—at least the following duties:

a. To exercise reasonable care in handling and using the Private Information in its care and custody;

b. To implementing industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. To promptly detect attempts at unauthorized access;

d. To notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their Private Information;

87. Also, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

88. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' Private Information.

89. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect consumers' Private Information. The FTC publications and orders promulgated under the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class Members' sensitive Private Information.

90. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as detailed *supra*. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

91. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class Members' PHI.

92. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

93. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant hold vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information—whether by malware or otherwise.

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

95. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered

or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

97. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

99. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class Members' Private Information.

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

101. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

102. The harm resulting from the Data Breach was the type of harm that HIPAA and the FTC Act were intended to guard against. And Plaintiff and Class Members are within the classes of persons that these statutes aim to protect.

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

104. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

105. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

106. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of receiving payment from Defendant. Plaintiff and Class Members provided their Private Information to Defendant or its third-party agents in exchange for Defendant's employment.

107. Plaintiff and the Class Members accepted Defendant's offers by disclosing their Private Information to Defendant or its third-party agents in exchange for employment.

108. In turn, and through internal policies, Defendant agreed to protect and not disclose the Private Information to unauthorized persons.

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

110. After all, Plaintiff and Class Members would not have entrusted their Private Information to Defendant or its third-party agents in the absence of such an agreement with Defendant.

111. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

113. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

a. Failing to safeguard their information;

b. Failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. Failing to comply with industry standards;

d. Failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. Failing to ensure the confidentiality and integrity of the electronic Private Information that Defendant created, received, maintained, and transmitted.

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

115. Defendant's material breaches were the direct and proximate cause of Plaintiff and Class Members' injuries (as detailed *supra*).

116. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

117. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

118. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

119. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their Private Information.

120. Because of the highly sensitive nature of the Private Information, Plaintiff and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

121. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

122. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff and Class Members' Private Information.

123. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and or warn Plaintiff and Class Members of the Data Breach.

124. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff and Class Members' Private Information.

125. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered—and will continue to suffer—injury, including but not limited to:

a. Actual identity theft;

b. The compromise, publication, and/or theft of their Private Information;

c. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

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

e. The continued risk to their Private Information, which remains in 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 their continued possession;

f. Future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

g. The diminished value of Defendant's services they received.

126. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
Intrusion upon Seclusion/Invasion of Privacy
(On Behalf of Plaintiff and the Class)

127. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

128. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the Restatement (Second) of Torts' formulation:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts§ 652B (1977).

129. Plaintiff and Class Members had a reasonable expectation of privacy in their Private Information which Defendant controlled.

130. Defendant's conduct as alleged above intruded upon Plaintiff and Class Members' seclusion under common law.

131. By intentionally failing to keep Plaintiff and Class Members' Private Information sufficiently secure, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

132. Defendant knew that an ordinary person in Plaintiff's or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

133. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

134. Defendant intentionally concealed from and delayed reporting to Plaintiff and Class Members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

135. The conduct described above was at or directed at Plaintiff and the Class Members.

136. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff and Class Members' protected privacy interests causing anguish and suffering such that

an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

137. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

SIXTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

138. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

139. This claim is pleaded in the alternative to the breach of implied contract claim.

140. Plaintiff and Class Members conferred a benefit upon Defendant. And Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members.

141. Defendant benefitted by using their Private Information to more easily—and thus more cheaply—provide employment and then pay for said employment.

142. Plaintiff and Class Members have no adequate remedy at law.

143. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class Members' Private Information because Defendant failed to adequately protect it.

144. Defendant unjustly enriched itself by cutting the costs it reasonably should have invested on data security to secure Plaintiff's and Class Members' Personal Information. Rather, Defendant decided to increase its profits—at the expense of Plaintiff and Class Members—by utilizing cheaper, ineffective security measures. Thus, Plaintiff and Class Members suffered as a

direct and proximate result of Defendant's decision to prioritize its own profits over reasonable security.

145. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

146. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered—and will continue to suffer—injuries, including but not limited to:

a. Actual identity theft;

b. The loss of the opportunity of how their Private Information is used;

c. The compromise, publication, and/or theft of their Private Information;

d. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information;

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

f. The continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and

g. Future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information

compromised because of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

147. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

SEVENTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

148. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

149. 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. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

150. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

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

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class Members.

152. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

153. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

154. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff's and Class Members' injuries.

155. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

156. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and Class Members respectfully request judgment against Defendant and that the Court enter an order:

a. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

b. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

c. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

d. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

e. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

f. Awarding attorneys' fees and costs, as allowed by law;

g. Awarding prejudgment and post-judgment interest, as provided by law;

h. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

i. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: November 29, 2022

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3232 McKinney Avenue, Suite 700
Dallas, Texas 75204
Telephone: 214-744-3000
Facsimile: 214-744-3015
jkendall@kendalllawgroup.com

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com
brittanyr@turkestrauss.com

Attorneys for Plaintiff and the Proposed Class