UNITED STATES DISTRICT COURT FOR THE

WESTERN DISTRICT OF TEXAS

SAN ANTONIO DIVISION

Richard Charitat, on behalf of himself and all others similarly situated,	§	
***Plaintiff*,**	§	
	§	**Case No. 5:22-cv-862**
v.	§	
	§	
Pape-Dawson Engineers, Inc.	§	
	§	
***Defendant*.**	§	

PLAINTIFF'S ORIGINAL CLASS ACTION COMPLAINT

Plaintiff Richard Charitat ("Plaintiff"), individually and on behalf of all others similarly situated, brings this national Class Action Petition against Defendant Pape-Dawson Engineers, Inc. (hereinafter known as "Pape-Dawson" or "Defendant"), a Texas corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of counsel, facts that are a matter of public record and also will likely have further evidentiary support after a reasonable opportunity for further investigation or discovery.

I. NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack against Defendant Pape-Dawson that allowed a third party to access Defendant's computer systems and data, resulting in the compromise of highly sensitive personal information belonging to current and former employees of Pape-Dawson as well as to consumers (the "Data Breach"). Because of the Data Breach, Plaintiff and other victims ("Class Members") suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time

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

2. Upon information and believe, the information compromised in the Data Breach is confidential personally identifiable information of consumers and employees (collectively the "Private Information").

3. Plaintiff brings this class action lawsuit on behalf of 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 Plaintiff and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party or precisely what specific type of information was accessed.

4. On information and belief, 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 a cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's 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.

5. In addition, on information and belief, Defendant failed to properly monitor the computer network and IT systems that housed the Private Information.

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

7. Armed with the Private Information accessed in the Data Breach, data thieves can

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' names to obtain medical services, 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, which could foreseeably result in the erroneous arrest of class members in the future.

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

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

10. By his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

11. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

12. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract; (iii) negligence per se; (iv) breach of fiduciary duty; (v) intrusion upon seclusion/invasion of privacy and (vi) unjust enrichment.

II. PARTIES

Plaintiff

13. Plaintiff Richard Charitat is a natural person, who entrusted his Private Information to the Defendant. Defendant obtained and continues to maintain Plaintiff's Private Information, and Defendant owed him a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff would not have entrusted his Private Information to Defendant had he known that Defendant failed to maintain adequate data security. Plaintiff's Private Information was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

14. Plaintiff received a notice letter from Defendant dated June 21, 2022, stating that Pape-Dawson had experienced a cybersecurity event that my have affected "the privacy of your personal information." The letter stated that four months earlier, on February 21, 2022, Pape-Dawson became aware of suspicious activity on its servers. After an investigation, Pape-Dawson determined "an unauthorized actor potentially gained access to certain systems and certain information within those systems between February 21 and February 25, 2022."

15. The breach notice letter said that as of April 28, 2022, Pape-Dawson had completed a review of "potentially impacted data to identify individuals with information potentially at risk." The form letter Plaintiff received did not identify specifically what personal information of his had been compromised.

16. Defendant is a Texas corporation with its headquarters and principal place of business being located at 2000 NW Loop 410, San Antonio Texas, 78213. This location is in the San Antonio Division of the Western District of Texas.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C.

§ 1332(d)(2) in that (1) this action is a class action with more than one hundred (100) Class Members; (2) Defendant is a Texas corporation and is a citizen of Texas; (3) Plaintiff and all Class Members are United States citizens and at least one putative Class member[1] is a citizen of a state other than Texas thus satisfying the minimal diversity requirement of 28 U.S.C. § 1332(d)(2)(A); and (4) the matter in controversy exceeds the sum or value of $5,000,000 exclusive of interests and costs.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because Defendant is subject to the Court's exercise of personal jurisdiction, a substantial part of the events or omissions giving rise to the claim occurred in this District, and as noted above the Defendant's headquarters and principal place of business is in the San Antonio Division of the Western District of Texas.

IV. DEFENDANT'S BUSINESS

19. Defendant is an engineering firm that provides civil engineering, surveying, GIS and environmental services for public and private clients across Texas. Upon information and belief Defendant has more than 850 current employees and many more former employees whose Personal Information Defendant still possesses.

20. In the ordinary course of employment Defendant's employees must provide (and Plaintiff did provide) Defendant with Personal Information.

21. In the ordinary course of business, Defendant's customers must provide Defendant with Personal Information in order to receive Defendant's services.

22. Defendant agreed to and undertook legal duties to maintain the Personal Information entrusted to it by Plaintiff and Class Members safely, confidentially, and in

[1] According to the Attorney General of the state of Indiana, at least one putative class member is a citizen of Indiana: *See* https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/Data-Breach-year-to-date-Report.pdf at line 518.

compliance with all applicable laws.

23. Defendant held the Private Information of Plaintiff and Class Members.

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

25. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

26. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, and to make only authorized disclosures of this information.

V. THE CYBERATTACK

27. In late June of 2022, Defendant publicly disclosed that months earlier, on or about February 21, 2022 Defendant had detected "suspicious activity" on its IT servers. Defendant informed the public that after an investigation, Defendant determined that cybercriminals accessed its network for the period February 21-25, 2022. According to Defendant, it took until late April 2022 to determine whose Personal Information had been compromised. Inexplicably, Defendant took another three months to notify Data Breach victims by letter.

28. Upon information and belief, more than 10,000 individuals had their Private Information exposed in the Data Breach.

29. The Private Information contained in the files accessed by hackers was not encrypted.

30. Upon information and belief, the targeted Data Breach was expressly designed to

gain access to private and confidential data of Plaintiff and the Class Members.

31. Because of the Data Breach, data thieves were able to gain access to and hold hostage Defendant's IT systems and, were able to compromise, access, and acquire the protected Private Information of Plaintiff and Class Members.

32. Defendant had obligations created by contract law, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

34. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[2] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[3] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[4]

35. Indeed, cyberattacks 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 report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[5]

---

[2] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[3] *Id*.
[4] *Id*.
[5] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited July 31, 2022).

36. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[6]

37. 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 Fails to Comply with FTC Guidelines

38. 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.

39. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal 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.[7] 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.[8]

40. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction; limit access to

---

[6] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited July 31, 2022).

[7] 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 July 31, 2022).

[8] *Id*.

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.

41. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

43. Defendant was at all times fully aware of its obligation to protect the Private Information of persons who had provided it to Defendant, including its employees, former employees, and individuals whose personal information it maintained. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

44. Several best practices have been identified that at a minimum should be implemented by businesses 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 sensitive data.

45. Other best cybersecurity practices that are standard 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.

46. 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.

47. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

VI. DEFENDANT'S NEGLIGENT ACTS AND BREACH

48. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect employees' and consumers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's

networks, and to maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

g. Failing to adhere to industry standards for cybersecurity.

49. As the result of antivirus and malware protection software in dire need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks, Defendant negligently and unlawfully failed to safeguard Plaintiff' and Class Members' Private Information by allowing cyberthieves to access Defendant's IT systems and remove data which contained unsecured and unencrypted Private Information.

50. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

51. Data breaches are problematic because the breaches can negatively impact the overall daily lives of individuals affected by the attack.

52. The United States Government Accountability Office 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."[9]

[9] *See* U.S. Gov. Accounting Office, GAO-07-737, "Personal Information: Data Breaches Are Frequent, but Evidence

53. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, taking over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, 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 otherwise harass or track the victim. 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 individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

54. The FTC recommends that identity theft 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 (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.[10]

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

56. Identity thieves can also use Social Security numbers to obtain a driver's license or

---

of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" (GOA, 2007). Available at https://www.gao.gov/new.items/d07737.pdf. (last visited July 31, 2022).

[10] *See* IdentityTheft.gov, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited July 31, 2022).

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.

57. Moreover, theft of Private Information results in the loss of a valuable property right.[11]

58. Its value is axiomatic, considering the value of "big data" in corporate America and the fact 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.

59. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and between when Private Information and/or financial information is stolen and when it is used.

60. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [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.

See GAO Report, at p. 29.

[11] *See*, *e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, 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).

61. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

62. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

63. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

64. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[12] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

65. 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.[13] 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.[14] 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 employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an

[12] *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 July 31, 2022).
[13] Identity Theft and Your Social Security Number, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 31, 2022).
[14] *Id*. at 4.

individual's authentic tax return is rejected.

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

67. 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."

68. 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."

69. Medical information is especially valuable to identity thieves.

70. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[15] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[16]

71. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

72. For this reason, Defendant knew or should have known about these dangers and strengthened its data security accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

VII. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

[15] *See* Omri Toppol, Email Security: How You Are Doing It Wrong & Paying Too Much, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last visited July 31, 2022).
[16] *See* Vaas, Cyberattacks, *supra*, n. 28.

73. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant has merely offered Plaintiff and Class Members 24 months of fraud and identity monitoring services, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach. Signing up for this service requires Plaintiff and Class Members to forfeit time that could otherwise be spent making money or enjoying life. Moreover, it is unclear when the credit monitoring service will be rescinded, at which point Plaintiff and Class Members will be required to pay for credit monitoring services out of their own pocket because once Private Information is stolen the threat of misuse continues for the remainder of the victim's life.

74. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

75. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

76. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

77. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

78. In fact, Plaintiff has already incurred approximately $150.00 in out-of-pocket expenses related to the additional credit monitoring he purchased as a result of this breach.

79. Plaintiff has already suffered harm from Defendant's failure to safeguard his personal information. Following the breach of Defendant's system, Plaintiff received a notification from Experian that his personal information had been published on the dark web.

80. Plaintiff and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of their Private Information, a form of property that Defendant obtained from Plaintiff and Class Members; (b) violation of their privacy rights; and (c) actual, imminent, and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

81. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims, including Plaintiff, suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
b. Purchasing credit monitoring and identity theft prevention;
c. Placing "freezes" and "alerts" with reporting agencies;
d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their name;
e. Contacting financial institutions and closing or modifying financial accounts;

and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

82. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

Plaintiff's Experience

83. Until 2016, Plaintiff was an employee of Defendant.

84. As a condition of his employment, Plaintiff entrusted confidential information such as name, address, date of birth, Social Security number and other personally identifiable information to Defendant with the reasonable expectation and understanding that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to him.

85. Plaintiff received a notice from Defendant dated on or about June 21, 2022 informing him that the Private Information he entrusted to Defendant had been subject to unauthorized access by an unknown cyber attacker.

86. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

87. As a result of the Data Breach, Plaintiff spent approximately $150 on credit monitoring services through Experian, and Experian informed him that his Private Information is on the dark web.

88. Plaintiff has also spent a significant number of hours reviewing his accounts and contacting other businesses and will continue to spend valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

89. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights;(c) the likely theft of his Private Information and (d) actual, imminent, and impending injury arising from the increased risk of identity theft and fraud.

90. Plaintiff has also suffered emotional distress as a result of the release of his Private Information and its publication on the dark web. which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

91. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

VIII. CLASS ACTION ALLEGATIONS

92. Plaintiff brings this action on behalf of himself and all other persons similarly

situated.

93. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons whose Private Information was compromised as a result of the Data Breach, for which Defendant provided notice in June 2022 (the "Class").**

94. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

95. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification.

96. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiff at this time.

97. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff' and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

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

f. Whether Defendant breached its duty to Plaintiff and Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Plaintiff and Class Members' Private Information in the Data Breach;

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

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was per se negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

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

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

98. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

99. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

100. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

101. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action

as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

102. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

103. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

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

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

104. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

IX. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

105. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

106. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain employment. Defendant also collected consumers' Private Information in the course of its business.

107. By collecting and storing this data in Defendant's computer property, 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 Plaintiff's 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 their security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

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

109. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees, and Defendant and its customers, which is recognized by laws and regulations as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

110. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

111. 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.

112. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and 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 Plaintiff's and Class Members' Private Information;

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

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

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

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

f. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

113. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and 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.

114. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in one or more types of injuries to Class Members.

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

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

117. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

118. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

119. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for employment, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information. And when consumers provided their Private Information to Defendant in exchange for receiving Defendant's services, they did so with the belief that Defendant had agreed to reasonably protect such information.

120. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

121. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

122. Plaintiff and Class Members provided labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so. Class Members similarly paid money to Defendant for its services with the reasonable belief and expectation that Defendant would use part of that payment to obtain adequate data security for the Private Information consumers entrusted to Defendant. Defendant failed to do so.

123. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

124. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

125. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

126. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

127. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

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

129. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring

procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT
NEGLIGENCE PER SE
(On Behalf of Plaintiff and All Class Members)

130. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

131. Pursuant to 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's and Class Members' Private Information.

132. 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's and Class Members' Private Information.

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

134. 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.

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

136. 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.

FOURTH COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

137. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

138. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's 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.

139. 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, in particular, to keep secure their Private Information.

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

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

142. 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.

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

144. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) 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; (v) 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; (vi) 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 (vii) the diminished value of Defendant's services they received.

145. 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 COUNT
INTRUSION UPON SECLUSION/INVASION OF PRIVACY

(On Behalf of Plaintiff and All Class Members)

146. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

147. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> 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).

148. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information that Defendant mishandled.

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

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

a. Intentionally and substantially intruding into Plaintiff's 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.

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

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

153. 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.

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

155. As a proximate result of such intentional misuse and disclosures, Plaintiff 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's 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.

156. 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 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 COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

157. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

158. Plaintiff brings this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of implied contract count, the second count listed in this Complaint.

159. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including money it earns through work performed by Plaintiff and the Class Members and money paid to it by consumers in exchange for its services.

160. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

161. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they performed work for and Defendant and on Defendant's behalf and in so doing provided Defendant with their Private Information. Class members also conferred

a monetary benefit in the form of payments to Defendant for its services and also entrusted Defendant with their Private Information In exchange, Plaintiff and Class Members should have received from Defendant compensation in the form of adequate data security designed to safeguard their Private Information.

162. Defendant knew that Plaintiff and Class Members conferred a benefit and Defendant accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

163. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

164. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to use that money to implement appropriate data management and security measures that are mandated by industry standards.

165. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

166. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

167. 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.

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

169. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, 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 as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

X. JURY TRIAL DEMANDED

172. Plaintiff demands a trial by jury on all claims so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff 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 personal identifying information of Plaintiff 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 Plaintiff 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 Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff 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 employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff 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 employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' 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;

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

D. For an award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

Dated: August 8, 2022

Respectfully submitted,

s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

GARY M. KLINGER*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

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

ATTORNEYS FOR PLAINTIFF

***Pro Hac Vice Forthcoming**

ClassAction.org
