UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

JESSE JAMES PAGAN, LILYANN DAVILA, and JACK COWAN *on behalf of themselves and all similarly situated persons*,	:	
Plaintiffs,	:	
v.	:	Civil Action No. 3:22-cv-297
FANEUIL, INC.,	:	
Defendant.	:	

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs Jesse James Pagan, Lilyann Davila and Jack Cowan ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Class Action Complaint (the "Action") against Faneuil, Inc. ("Defendant" or "Faneuil"), a Virginia-based corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This Action arises out of the recent ransomware attack and data breach at Faneuil that targeted the information of past and present employees who worked at Faneuil (the "Data Breach").

2. The Data Breach resulted in unauthorized access to the sensitive data of past and present employees that worked at Faneuil. Because of the Data Breach, thousands of Class Members' suffered ascertainable losses inclusive of out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack. In addition, Plaintiffs and Class

Members are now faced with the present and substantial risk of imminent harm caused by the compromise of their sensitive personal information, including their names, addresses at the time of employment, Social Security numbers, phone numbers, and email addresses (hereinafter, the "Personally Identifiable Information" or "PII").

3. Even worse, after discovering the Data Breach, Faneuil sat on the information for nearly half a year – failing to disseminate data breach consumer notifications until February 1, 2022. When a data set that is inclusive of the aforementioned PII is breached, every moment is precious to ensure that that data is not then weaponized against the rightful owner of that data through identity theft. Sitting on this information diminished the Data Breach victims' chances at mitigating the consequences resulting from Faneuil's failure to provide adequate protection of the sensitive and private information it chose to maintain for its own financial benefit and allowed Faneuil to dodge responsibility, inevitably worsening the Data Breach victims' chances at weathering the storm that Faneuil created.

4. As a result of the Data Breach, Plaintiffs and Class Members have been harmed – they have been exposed to a heightened present and continuing risk of fraud and identity theft. Plaintiffs and Class Members must now and forever closely monitor their financial accounts to guard against identity theft.

5. Plaintiffs and Class Members may also incur out-of-pocket costs, for example, through having to purchase identity theft protection systems, credit freezes, or other protective measures to deter and detect identity theft. Plaintiffs seek to remedy those harms on behalf of themselves and all similarly situated persons whose PII was accessed unlawfully during the Data Breach. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement for out-of-pocket costs, and injunctive relief including improvements to

Defendant's data security systems and protocols, future annual SOC 2 audits, annual assessments by a qualified independent third party assessor to ensure that Defendant is complying with the injunctive relief components imposed by the Court and adequate identity theft protection services funded by the Defendant.

6. In the notices sent to Plaintiffs and Class Members, Defendant recognized that each Class Member is now subject to the present and continuing risk of identity theft and fraud: Defendant offered Plaintiffs and Class Members identity theft protection from Experian. The Defendant offered services for only two years, however, which is insufficient to protect Plaintiffs and Class Members from the lifelong implications of having their sensitive PII accessed, acquired, exfiltrated, and/or published on the internet. As another element of damages, Plaintiffs and Class Members seek a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protective services for their respective lifetimes.

7. Consequently, Plaintiffs bring this Action against Defendant seeking redress for its unlawful conduct, asserting claims for: 1) Negligence; 2) Breach of Implied Contract; 3) Unjust Enrichment; and 4) Violations of California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq* ("CCPA").

II. JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act because (1) there are more than 100 putative Class Members, (2) the aggregate amount-in-controversy, exclusive of costs and interest, exceeds $5,000,000.00, and (3) there is minimal diversity because Plaintiffs and Defendant are citizens of different states – namely, that Plaintiffs are Florida and California residents and citizens and the Defendant is headquartered here, in Virginia.

9. This Court has personal jurisdiction over the Defendant because the Defendant is headquartered in this District. Additionally, this Court has personal jurisdiction over the Defendant because they have substantial contacts with this District and have purposely availed themselves to the Courts in this District.

10. In accordance with 28 U.S.C. 1391, venue is proper in this District because a substantial part of the conduct giving rise to the Plaintiffs' claims occurred in this District, the Defendant is headquartered in this District, and the Defendant transacts business within this District.

III. PARTIES

11. Plaintiff Jesse James Pagan: Plaintiff Pagan is a resident and citizen of the state of Florida and was notified of the Data Breach and his PII being compromised by way of a data breach notification letter disseminated by Defendant on or about February 1, 2022. The letter notified Plaintiff that on August 18, 2021, Faneuil experienced a ransomware attack whereby its servers were accessed by unauthorized actors and that certain PII was included in files that those unauthorized actors accessed and copied.

12. Plaintiff Lilyann Davila: Plaintiff Davila is a resident and citizen of the state of Florida and was notified of the Data Breach and her PII being compromised by way of a data breach notification letter disseminated by Defendant on or about February 1, 2022. The letter notified Plaintiff that on August 18, 2021, Faneuil experienced a ransomware attack whereby its servers were accessed by unauthorized actors and that certain PII was included in files that those unauthorized actors accessed and copied.

13. Plaintiff Jack Cowan: Plaintiff Cowan is a resident and citizen of the state of California and was notified of the Data Breach and that his PII was compromised by way of a data

breach notification letter he received on or about February 1, 2022. The letter notified Plaintiff that on August 18, 2021, Faneuil experienced a ransomware attack whereby its servers were accessed by unauthorized actors and that certain PII was included in files that those unauthorized actors accessed and copied.

14. Defendant Faneuil, Inc.: Defendant Faneuil, Inc. is a Delaware corporation, engaging in logistics and business solutions with a principal place of business in Hampton, Virginia.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

15. According to Defendant, "Faneuil provides a broad array of business process outsourcing solutions . . . and currently employs more than 5,500 professionals nationwide."[1]

16. According to Defendant's Data Breach Notification letter, with respect to data privacy, "we value the trust that individuals place in us with their information and we understand the importance of protecting the information that we maintain."

17. On information and belief, in the course of collecting PII from consumers and employees including Plaintiff, Defendant promised to provide confidentiality and adequate security for customer and employee data through their applicable privacy policy and through other disclosures.

18. By obtaining, collecting, using and deriving benefits from Plaintiffs and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting said PII from unauthorized disclosure.

[1] **https://www.faneuil.com/about-us/** (last accessed Aug 10, 2022).

19. Plaintiffs and the Class Members reasonably relied (directly or indirectly) on this sophisticated company to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Employees, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

20. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

21. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

22. Contrary to Defendant's duty and to its representations that it values "the trust that individuals place in us with their information and we understand the importance of protecting the information that we maintain," Defendant failed to respect and protect consumer privacy.

THE DATA BREACH

23. In February 2022, Defendant first began notifying Class Members and state AGs about a widespread data breach of its computer systems involving the sensitive PII of consumers. According to Defendant, the breach occurred in August of 2021.

24. According to Faneuil's Data Breach Notification, a ransomware attack was discovered on August 18, 2021.[2]

---

[2] Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid. While at one time the prime motive of a ransomware attack was simply to encrypt a user's data and hold it for ransom, ransomware attacks are now primarily the last phase of a multi-pronged cyberattack that is targeted at confidential data, and that has as its prime motivation the theft of confidential data like the PII stolen here. A recent analysis shows that data exfiltration occurs in 70 percent of all ransomware attacks. Jessica Davis, *70% Ransomware Attacks Cause Data Exfiltration; Phishing Top Entry Point*, HealthITSecurity (Feb. 3, 2021), *available at*: **https://healthitsecurity.com/news/70-ransomware-attacks-cause-data-exfiltration-phishing-top-entry-point** (last accessed Aug. 10, 2022).

25. Following the incident, Defendant conducted a review of its files and ultimately determined that there had been a data breach involving Plaintiffs' and Class Members' PII.

26. Defendant's investigation and notification letter confirmed the worst: "the attackers accessed and copied certain company records, including records of past and present Faneuil employees." According to Defendant, the PII accessed and stolen in the Data Breach included names, addresses at the time of employment, Social Security numbers (the holy grail for identity thieves), and email addresses.

27. Even worse, rather than promptly informing Class Members about the Data Breach so they could take measures to protect themselves, Defendant opted not to inform consumers until *nearly six months* after the discovery of the Data Breach on February 1, 2022.

28. The Data Breach resulted in unauthorized access to the sensitive data of current and former Faneuil employees. Because of the Data Breach, thousands of Class Members' suffered ascertainable losses including out-of-pocket expenses and the value of their time incurred to mitigate the effects of the attack and the present and imminent harm caused by the compromise of their sensitive personal information.

29. The Personally Identifiable Information contained in the files accessed in the Data Breach was not encrypted or redacted.[3]

30. Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and the mutual understanding that Defendant would comply with its obligations to

[3] It is clear that the information exposed in the Data Breach was unencrypted: California law requires companies to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1) (emphasis added). Defendant notified the California Attorney General of the Data Breach on or about Feb. 1, 2022, evidencing that the exposed data was unencrypted. *See* **https://oag.ca.gov/ecrime/databreach/reports/sb24-550731** (last accessed Aug. 10, 2022).

implement and utilize adequate data security measures to keep such information confidential and secure from unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the breach.

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

SECURING PII AND PREVENTING DATA BREACHES

32. Defendant could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

33. In its notice letters, Defendant acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, and protecting the PII of employees and former employees is vital to virtually all of Defendant's business purposes as a firm employing over 5,500 individuals. Defendant has acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

THE DATA BREACH WAS A FORESEEABLE RISK OF WHICH DEFENDANT WAS ON NOTICE

34. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

35. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[4]

36. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

37. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."

38. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estée Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

---

[4] *See* https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-savs/ (last accessed Aug. 10, 2022)

39. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

40. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgements of data security compromises, and despite their own acknowledgement of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

DEFENDANT, AT ALL RELEVANT TIMES, HAD A DUTY TO PLAINTIFFS AND CLASS MEMBERS TO PROPERLY SECURE THEIR PRIVATE INFORMATION

41. At all relevant times, Defendant had a duty to Plaintiffs and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, use available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to *promptly* notify Plaintiffs and Class Members when Defendant became aware that their PII may have been compromised.

42. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

43. Security standards commonly accepted among businesses, and that Defendant lacked, include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs;

j. Monitoring for server requests from Tor exit nodes;

k. The destruction of Class Members' data where Defendant no longer has an authorized need for the retention of that data; and

l. An appropriate management structure to ensure oversight of Defendant's information security posture, and to address deficiencies when detected and to ensure the proper funding to maintain a secure environment.

44. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[5] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

THE VALUE OF PERSONALLY IDENTIFIABLE INFORMATION

45. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity

[5] 17 C.F.R. § 248.201 (2013).

credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[7]

46. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent users and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

47. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[8]

---

[6] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: **https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/** (last accessed Aug. 5, 2022).

[7] *Dark Web Price Index 2021,* Zachary Ignoffo, March 8, 2021, *available at:* **https://www.privacyaffairds.com/dark-web-price-index-2021/** (last accessed Aug. 5, 2022).

[8] Social Security Administration, *Identity theft and Your Social Security Number, available at:* https//www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Aug. 5, 2022).

48. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventative action to defend against the possibility of misuse of a Social Security number is not permitted: an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

49. 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."[9]

50. PII Can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[10]

51. Given the nature of Defendant's Data Breach, as well as the extreme delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' PII can easily obtain Plaintiffs' and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

52. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

---

[9] Brian Naylor, *Victims of Social Security Number Theft Find it's Hard to Bounce Back,* NPR (Fed. 9, 2015), **http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft** (last accessed Aug. 5, 2022).

[10] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers,* Computer World (Feb. 6, 2015), **http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credt-card-numbers.html** (last accessed Aug. 5, 2022).

breach, because credit card victims can cancel or close credit and debit card accounts.[11] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

53. To date, Defendant offered its consumers only two years of identity monitoring services. The offered services are inadequate to protect Plaintiffs and Class Members from the threats they face presently and for years to come, particularly in light of the sensitive PII at issue here.

54. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures.

DEFENDANT FAILS TO FOLLOW FTC GUIDELINES

55. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses to 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.

56. 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 patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any

[11] *See* Jesse Damani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar. 25, 2020, *available at:* **https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513fl** (last accessed Aug. 5, 2022)

security problems.[12] 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.[13]

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

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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.

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

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

---

[12] 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 6, 2022).

[13] *Id.*

61. Defendant was at all times fully aware of its obligation to protect the Personally Identifiable Information of its subjects. Defendant was also aware of the significant repercussions that would result from its failure to do so.

62. Several best practices have been identified that at a minimum should be implemented by companies 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.

63. Other best cybersecurity practices that are standard in the Defendant's industry, and that upon information and belief Defendant did not employ, 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.

64. 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.

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

DEFENDANT'S BREACH

66. Defendant breached its obligations to Plaintiffs 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 consumers' PII;

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

d. Failing to train its employees in the proper handling of data breaches, the protection of PII, and the maintenance of adequate email security practices;

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

f. Failing to adhere to industry standards for cybersecurity.

67. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its IT systems which contained unsecured and unencrypted PII.

68. Accordingly, as outlined below, Plaintiffs and Class Members now face present fraud and identity theft and an increased risk of fraud and identity theft for the rest of their lives. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant.

HARM TO CONSUMERS

69. PII 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.

70. 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 Plaintiffs and Class Members are at a present and an increased risk of fraud and identity theft for many years into the future.

71. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

72. 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. 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. 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 individual's authentic tax return is rejected.

73. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he

credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

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

75. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personally Identifiable Information is stolen and when it is used.

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

77. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems 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.

HARM TO PLAINTIFFS

A. HARM TO PLAINTIFF PAGAN

78. Before the Data Breach, Mr. Pagan provided his PII to Faneuil as a requirement for employment with the company. Mr. Pagan would have never provided his PII to Faneuil had he known it lacked adequate data security.

---

[14] Brian Naylor, "*Victims of Social Security Number Theft Find It's Hard to Bounce Back*," NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about- identity-theft (last visited Aug. 5, 2022).

79. In February, 2022, Mr. Pagan received a Notice of Data Breach letter from Faneuil informing him that his full name and Social Security number, amongst other information, was stolen by cyberthieves in the Data Breach. As a result of the Data Breach, Faneuil directed Plaintiff Pagan to take certain steps to protect his PII and otherwise mitigate his damages.

80. As a result of the Data Breach and the directives that he received in the Notice Letter, Mr. Pagan has spent significant time and resources dealing with the Data Breach and continues to this day spending time dealing with the consequences of the Data Breach, including, but not limited to, self-monitoring his bank and credit card accounts, verifying the legitimacy of the *Notice of Data Breach*, communicating with his bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

81. Mr. Pagan is very careful about sharing his own PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

82. Mr. Pagan stores any and all documents containing PII in a secure location, and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

83. Mr. Pagan suffered actual injury and damages due to Faneuil's inadequate measures to safeguard his PII before the Data Breach.

84. Mr. Pagan suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to Faneuil for the purpose of providing employment, which was compromised in and as a result of the Data Breach.

85. Mr. Pagan suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered anxiety and increased concerns for the theft of his privacy

since he received the Notice Letter. He is especially concerned about the theft of his full name paired with his Social Security number.

86. Mr. Pagan has suffered present, imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and criminals.

87. Mr. Pagan has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Faneuil's possession, is protected and safeguarded from future breaches.

B. HARM TO PLAINTIFF DAVILA

88. Before the Data Breach, Ms. Davila provided her PII to Faneuil as a requirement for employment with the company. Ms. Davila would have never provided her PII to Faneuil had she known it lacked adequate data security.

89. In February, 2022, Ms. Davila received Notice of Data Breach Letter from Faneuil informing her that her full name and Social Security number, amongst other information, was stolen by cyberthieves in the Data Breach. As a result of the Data Breach, Faneuil directed Plaintiff Davila to take certain steps to protect her PII and otherwise mitigate her damages.

90. As a result of the Data Breach and the directives that she received in the Notice Letter, Ms. Davila has spent significant time and resources dealing with the Data Breach and continues to this day spending time dealing with the consequences of the Data Breach, including, but not limited to, self-monitoring her bank and credit card accounts, verifying the legitimacy of the *Notice of Data Breach*, communicating with her bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

91. Ms. Davila is very careful about sharing her own PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

92. Ms. Davila stores any and all documents containing PII in a secure location, and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

93. Ms. Davila suffered actual injury and damages due to Faneuil's mismanagement of her PII before the Data Breach.

94. Ms. Davila suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to Faneuil for the purpose of providing her employment, which was compromised in and as a result of the Data Breach.

95. Ms. Davila suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered anxiety and increased concerns for the theft of her privacy since she received the Notice Letter. She is especially concerned about the theft of her full name paired with her Social Security number.

96. Ms. Davila has suffered present, imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

97. Ms. Davila has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Faneuil's possession, is protected and safeguarded from future breaches.

C. HARM TO PLAINTIFF COWAN

98. Before the Data Breach, Mr. Cowan provided his PII to Faneuil as a requirement for employment with the company in or about October 2019 to April 2020. Mr. Cowan would have never provided his PII to Faneuil had he known it lacked adequate data security.

99. In February, 2022, Mr. Cowan received Notice of Data Breach Letter from Faneuil informing him that his full name and Social Security number, amongst other information, was stolen by cyberthieves in the Data Breach. As a result of the Data Breach, Faneuil directed Plaintiff Cowan to take certain steps to protect his PII and otherwise mitigate his damages.

100. As a result of the Data Breach and the directives that he received in the Notice Letter, Mr. Cowan has spent significant time and resources dealing with the Data Breach and continues to this day spending time dealing with the consequences of the Data Breach, including, but not limited to, self-monitoring his bank and credit card accounts, verifying the legitimacy of the *Notice of Data Breach*, communicating with his bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

101. Mr. Cowan purchased credit monitoring for a discounted rate of $59 per year from Experian.

102. Mr. Cowan has experienced multiple instances of credit and debit card fraud since late 2021, totaling over $250. Mr. Cowan has so far been reimbursed by his bank and credit card companies.

103. Mr. Cowan is very careful about sharing his PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

104. Mr. Cowan shreds any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and

financial accounts. Moreover, he diligently chooses unique usernames and passwords for her various online accounts.

105. Mr. Cowan suffered actual injury and damages due to Faneuil's mismanagement of her PII before the Data Breach.

106. Mr. Cowan suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that she entrusted to Faneuil for the purpose of providing him employment, which was compromised in and as a result of the Data Breach.

107. Mr. Cowan suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered anxiety and increased concerns for the theft of him privacy since he received the Notice Letter. He is especially concerned about the theft of his full name paired with his Social Security number.

108. Mr. Cowan has suffered present, imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

109. Mr. Cowan has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Faneuil's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

110. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose Personally Identifiable Information was maintained on Faneuil's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Nationwide Class").
>
> All persons residing in California whose Personally Identifiable Information was maintained on Faneuil's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "California Sub-Class," collectively with the "Nationwide Class," the "Class").

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

112. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of over 100 individuals whose sensitive data was compromised in the Data Breach.

113. **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 the Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Personally Identifiable 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, during, and after the Data Breach complied with the 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, as applicable;

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

f. Whether Defendant breached a duty to Class Members to safeguard their Personally Identifiable Information;

g. Whether computer hackers obtained Class Members Personally Identifiable Information in the Data Breach;

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

i. Whether the Plaintiffs and Class Members suffered legally cognizable injuries as a result of the Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

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

l. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and/or injunctive relief;

114. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

115. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating Class actions.

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

117. **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 ofeach Class Member.

118. 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.

VI. CAUSES OF ACTION

FIRST COUNT

NEGLIGENCE
(On behalf of Plaintiffs and the Class)

119. Plaintiffs reallege and incorporate by reference all of the allegations contained in paragraphs 1 through 118.

120. Plaintiffs bring this count on behalf of themselves and the Class.

121. Faneuil required Plaintiffs and Class Members to submit non-public Personally Identifiable Information, including but not limited to, Social Security Numbers, as a condition of employment at Faneuil.

122. Plaintiffs and Class Members entrusted Defendant with their PII on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

123. By collecting and storing this data, and sharing it and using it for commercial gain, Faneuil had and/or voluntarily undertook a duty of care to use reasonable means to secure and safeguard this information, to prevent disclosure of the information, and to guard the information from theft.

124. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

125. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII entrusted to it involved an unreasonable risk of harm to Plaintiffs and Class Members, including harm that foreseeably could occur through the criminal acts of a third party.

126. Defendant owed a common law duty to Plaintiffs and Class to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This common law duty includes, among

other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs′ and Class Members′ information in Defendant's possession was adequately secured and protected.

127. Defendant's common law duty it owed to Plaintiffs and the Class included the duty to exercise appropriate clearinghouse practices to remove PII belonging to persons who transacted with its former customers that Defendant was no longer required to retain pursuant to regulations.

128. Defendant's common law duty it owed to Plaintiffs and the Class included the duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Class.

129. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII, a mandatory step in obtaining employment from Defendant.

130. Defendant was subject to an independent duty, untethered to any contract between Defendant and Plaintiffs and the Class to maintain adequate data security.

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

132. Plaintiffs and the Class were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance

of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems.

133. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendant to take reasonable measures to protect Plaintiffs' and the Class's PII and is a further source of Defendant's duty to Plaintiffs and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to implement and use reasonable measures to protect PII. Defendant, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. By failing to implement and use reasonable data security measures, Defendant acted in violation of § 5 of the FTCA.

134. Defendant is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendant to exercise reasonable care with respect to Plaintiffs and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiffs and the Class. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, Defendant was the only entity capable of adequately protecting the data that it collected and stored.

135. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendant′s wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant′s misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiffs′ and the Class's PII, including basic encryption techniques available to Defendant.

136. Plaintiffs and the Class had no ability to protect their PII that was in, and remains in, Defendant's possession.

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

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

139. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

140. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiffs and the Class by failing to implement at a very minimum the standard industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Class when the PII was within Defendant′s possession or control.

141. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

142. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the confidential PII entrusted to it in the face of increased risk of theft.

143. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination the PII entrusted to it.

144. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII belonging to persons who transacted with its former employees, and that Defendant was no longer required to retain pursuant to regulations.

145. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

146. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiffs and the Class would not have been compromised.

147. There is a close causal connection between (a) Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Class and (b) the harm or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs′ and the Class Members′ PII was accessed and exfiltrated as the direct and proximate result of Defendant′s failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

148. As a direct and proximate result of Defendant′s negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, 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 Plaintiffs′ and Class Members ′ PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members.

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

150. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, 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 PII in its continued possession.

151. As a direct and proximate result of Defendant′s negligence, Plaintiffs are now at an increased risk of identity theft or fraud.

152. As a direct and proximate result of Defendant′s negligence, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

SECOND CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

153. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

154. When Plaintiffs and Class Members provided their PII to Faneuil in exchange for employment, they entered into implied contracts with Faneuil pursuant to which Faneuil agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

155. Faneuil solicited and invited prospective and current employees to provide their PII as part of its regular business practices. These individuals accepted Faneuil's offers and provided their Information to Faneuil. In entering into such implied contracts, Plaintiffs and the Class reasonably presumed that Faneuil's data security practices and policies were reasonable and consistent with industry standards, and that Faneuil would use part of the funds received from Plaintiffs' and the Class's labor to pay for adequate and reasonable data security practices.

156. Plaintiffs and the Class would not have provided and entrusted their Information to Faneuil in the absence of the implied contract between them and Faneuil to keep the information secure.

157. Plaintiffs and the Class fully performed their obligations under the implied contracts with Faneuil.

158. Faneuil breached its implied contracts with Plaintiffs and the Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their PII was compromised as a result of a data breach.

159. As a direct and proximate result of Faneuil's breaches of their implied contracts, Plaintiffs and the Class sustained actual losses and damages as described herein.

THIRD CAUSE OF ACTION

UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

160. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

161. Plaintiffs bring this count on behalf of themselves and the Class in the alternative to the other Counts alleged herein to the extent necessary.

162. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of labor services and their PII.

163. Defendant collected, maintained, and stored the PII of Plaintiffs and Class Members and, as such, Defendant had knowledge of the monetary benefits conferred by them.

164. The money that Defendant received from Plaintiffs' and Class Members' labor services should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII.

165. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

166. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiffs and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiffs' PII.

167. Under principles of equity and good conscience, Defendant should not be permitted to retain the money it received from Plaintiffs' and Class Members' labor services that should have been used to implement the data security measures necessary to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII.

168. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiffs' and Class Members' PII, Plaintiffs and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

169. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and the Class.

170. The benefit conferred upon, received and enjoyed by Defendant was not conferred gratuitously and it would be inequitable and unjust for Defendant to retain the benefit. Defendant is therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on Defendant as a result of its wrongful conduct.

FOURTH CAUSE OF ACTION

Violations of California's Consumer Privacy Act
Cal. Civ. Code § 1798.100, *et seq*. ("CCPA")
(On Behalf of Plaintiff Cowan and the California Sub-Class)

171. Plaintiff Cowan and the California Sub-Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 118.

172. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary

costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[15]

173. As a result, in 2018 the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

174. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

175. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

176. Plaintiff and the California Sub-Class are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

---

[15] *California Consumer Privacy Act (CCPA) Compliance*, https://buyergenomics.com/ccpa-complience/ (last visited July 5, 2022).

177. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners;"

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information;"

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

178. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff Cowan's and the California Class Members' unencrypted first and last names and Social Security numbers, among other information.

179. Plaintiff Cowan's and the putative California Class Members' PII were subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and Social Security number, was wrongfully taken, accessed, and viewed by unauthorized third parties.

180. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff and the California Class Members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on their server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff and the California Class Members' PII as a result of this attack.

181. Plaintiff Cowan and the California Sub-Class seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. This relief is important because Defendant still holds PII related to Plaintiff and the California Sub-Class. Plaintiff and the Class have an interest in ensuring that their PII is reasonably protected.

182. On June 17, 2022, Plaintiff provided Defendant with written notice by certified mail of Defendant's violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1).

183. Following a request for an extension of time to respond to Plaintiff Cowan's notice of violation, Defendant responded to Plaintiff Cowan's notice on July 20, 2022. In Defendant's response Defendant asserted, without evidence or proof, that it "cured" the above failures to implement reasonable security procedures to prevent unauthorized access of Plaintiff and Class Members' PII by discussing the post attack actions it allegedly took, which, did not retroactively cure the unauthorized access, as they provide little assurance that Plaintiff and California Sub-Class members PII isn't still in the hands of unauthorized third parties.

184. Defendant asserts in its response that the cybercriminals deleted the PII they took, but provides no evidence or proof to that effect and, as such, is telling Plaintiff and California Sub-Class members to rely on Defendant relying on the honesty of Cybercriminals.

185. Furthermore, none of the steps Defendant asserts in its response demonstrate an actual cure of its failures to implement reasonable security measures to protect Plaintiff and California Sub-Class members' PII as the steps it asserts it has taken are not sufficient to protect Plaintiff and California Sub-Class members' PII.

186. Defendant's response is wholly insufficient to demonstrate any "actual cure" of its failures to implement reasonable security to protect the information. For instance, defendant claimed that there had been "no allegations or reports of identity theft or fraud" despite Plaintiff Cowan's own experience, detailed supra, of fraud that resulted from Defendant's failures to implement reasonable security measures or to cure them. Quite simply put, had Defendant

"actually cured" its violation of the CCPA, Plaintiff Cowan would not have experienced the fraud he has experienced.

187. As Defendant has not "actually cured" the violation, Plaintiff seeks statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

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

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class members;

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

D. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

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

ii. requiring Defendant to protect, including through encryption, all data collected

through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

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

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

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all 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 Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its 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 PII 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;

E. Ordering Defendant to pay for a lifetime of credit monitoring services for Plaintiffs and the Class;

F. For an award of actual damages and compensatory damages, as allowable by law;

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

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

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

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

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

VIII. JURY TRIAL DEMAND

Jury trial is demanded by Plaintiffs and members of the putative Class.

DATED: August 31, 2022

Respectfully submitted,

By, */s/ Lee A. Floyd*

Lee A. Floyd, VSB #88459
Justin M. Sheldon, VSB #82632
BREIT BINIAZAN, PC
2100 East Cary Street, Suite 310
Richmond, Virginia 23223
Telephone: (804) 351-9040
Facsimile: (804) 351-9170
Lee@bbtrial.com
Justin@bbtrial.com

Jeffrey A. Breit, VSB #18876
Kevin Biniazan, VSB #92019
BREIT BINIAZAN, P.C.
Towne Pavilion Center II
600 22nd Street, Suite 402
Virginia Beach, Virginia 23451
Telephone: (757) 622-6000
Facsimile: (757) 670-3939
Jeffrey@bbtrial.com
Kevin@bbtrial.com

David K. Lietz (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

M. Anderson Berry (admitted *pro hac vice*)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com

CERTIFICATE OF SERVICE

I certify that on the 31st day of August, 2022, I electronically filed the foregoing with the Clerk of Court by using the CM/ECF system, which will send a notice of electronic filing to all counsel of record who are CM/ECF participants.

/s/ Lee A. Floyd
Lee A. Floyd