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

LAUREN TURNER *on behalf of herself and all similarly situated persons*, Plaintiff, v. FIVE GUYS ENTERPRISES, LLC, Defendant.	:	Civil Action No. 1:23-cv-40

CLASS ACTION COMPLAINT

Plaintiff Lauren Turner ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint (the "Action") against Five Guys Enterprises, LLC ("Defendant" or "Five Guys""), a Virginia-based 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 her own actions, the investigation of counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") of Defendant's job applicants and current and former employees. The PII, which is defined by federal law,[1] includes, but is not limited to, names and Social Security numbers.

[1] *See, e.g.,* 2 C.F.R. § 200.79.

2. This Action arises out of the recent information theft and data breach at Five Guys that targeted the information of past and present employees of Five Guys (the "Data Breach") prior to and through September 17, 2022.

3. Because of the Data Breach, Plaintiff and thousands of Class Members suffered ascertainable losses including out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack. In addition, Plaintiff 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 and Social Security numbers as of September 17, 2022 (hereinafter, the "Personally Identifiable Information" or "PII").

4. Prior to and through September 17, 2022, Defendant obtained the PII of Plaintiff and Class Members, including by collecting it directly from Plaintiff and Class Members.

5. Prior to and through September 17, 2022, Defendant stored the PII of Plaintiff and Class Members, unencrypted, in an Internet-accessible environment on Defendant's network.

6. On or before September 17, 2022, Defendant learned of a data breach on its network that occurred on or around September 17, 2022 (the "Data Breach").

7. Defendant determined that, during the Data Breach, an unknown actor accessed files containing the PII of Plaintiff and Class Members.

8. Over two months later, on or around December 29, 2022, Defendant began notifying various states Attorneys General of the Data Breach.[2]

9. On or around December 29, 2022, Defendant began notifying Plaintiff and Class Members of the Data Breach.

[2] Office of Maine Attorney General, *Data Breach Notifications*, https://apps.web.maine.gov/online/aeviewer/ME/40/26dcead1-f092-464d-89ae-34057af0082b.shtml (last accessed Jan. 10, 2023).

10. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII included name and Social Security number.

11. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

12. The PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, Defendant waited more than three months after the Data Breach occurred to report it to the states Attorneys General and affected individuals. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiff and Class Members of that information.

13. As a result of this delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

14. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective

security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

15. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

16. Consequently, Plaintiff brings 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) the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100, *et seq*.

II. PARTIES

17. Plaintiff Lauren Turner is a citizen and resident of California residing in Los Angeles, California.

18. Defendant is a Virginia corporation with a principal place of business in Lorton, Virginia.

19. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently

unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

20. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

21. 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 Plaintiff's claims occurred in this District, the Defendant is headquartered in this District, and the Defendant transacts business within this District.

22. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

23. This Court has personal jurisdiction over Defendant because Defendant has its principal places of business within this District.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Defendant's headquarters are located in this District, and it conduct much of its business through this District.

IV. FACTUAL ALLEGATIONS

Defendant's Business

25. Five Guys operates over 1,700 hamburger restaurants in every state in the United States and in many countries.[3]

26. Five Guys claims to offer career opportunities from work on the line to management opportunities.[4]

Background

27. Defendant required the PII of Plaintiff and Class Members, including Defendant's job applicants and current and former employees.

28. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

29. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

Data Breach

30. On or about December 29, 2022, Defendant sent Plaintiff and Class Members a notice of the Data Breach (the "Notice of Data Breach"[5]). Defendant informed Plaintiff and other Class Members that:

> Five Guys Enterprises, LLC ("Five Guys") understands the importance of protecting the information that we maintain. We are writing to inform you that we recently identified and addressed a security incident that may have involved your information. This letter explains the incident, measures we have taken, and some steps you may choose to take. We identified a security incident on September 17, 2022 that involved unauthorized access to files on a file server.

---

[3] *See https://restaurants.fiveguys.com/* (last visited on Jan. 10, 2023).
[4] *See* https://www.joinfiveguys.com/ (last visited on Jan. 10, 2023).
[5] Notice of Security Incident filed with Maine Attorney General, file:///C:/Users/MICHA/Downloads/Five%20Guys_ME%20App%20&%20Sample%20(1).pdf (last visited on Jan. 10, 2023).

> We immediately implemented our incident response plan, took steps to contain the activity, and launched an investigation. A cybersecurity firm that has assisted other companies in similar situations was engaged. We also notified law enforcement and are supporting its investigation.
>
> The investigation identified unauthorized access to files on our file server that occurred on September 17, 2022. We conducted a careful review of those files and, on December 8, 2022, determined that the files contained information submitted to us in connection with the employment process, including your name and Social Security number. 3 28. The Notice of Data Breach that Defendant sent to Plaintiff stated that Plaintiff's name and Social Security number were impacted during the Data Breach. 29. Defendant admitted in the Notice of Data Breach that an unauthorized actor accessed sensitive information about Plaintiff and Class Members, including name and Social Security number. 30. In response to the Data Breach, Defendant claims that it "immediately implemented our incident response plan, took steps to contain the activity, and launched an investigation."

31. In response to the Data Breach, Defendant claims that it "immediately implemented our incident response plan, took steps to contain the activity, and launched an investigation."[6]

32. The PII contained in the files accessed in the Data Breach was not encrypted or redacted and was, as Defendant admits, "improperly stored."[7]

33. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and the mutual understanding that Defendant would comply with its obligations to implement and use 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.

---

[6] *Id*.

[7] 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 Nov. 14, 2022, evidencing that the exposed data was unencrypted. *See* https://oag.ca.gov/ecrime/databreach/reports/sb24-559168 (last accessed Jan. 10 , 2023).

34. 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

35. Defendant could have prevented this Data Breach by properly encrypting their computer files containing PII. Five Guys is a large, multinational corporation with locations all over the world. It is a sophisticated enterprise, and it should have encrypted their computer files containing PII of job applicants as well as past and present employees.

36. In the first page of the Notice of Data Breach, Five Guys states, it "understands the importance of protecting the information that we maintain,"[8] yet it allowed names and Social Security numbers to be stolen.

The Data Breach was a Foreseeable Risk of Which Defendant Was on Notice

37. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers and other bad actors precisely because of its value and marketability to hackers and identity thieves.

38. 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.[9]

[8] Notice of Security Incident filed with Maine Attorney General, file:///C:/Users/MICHA/Downloads/Five%20Guys_ME%20App%20&%20Sample%20(1).pdf (last visited on Jan. 10, 2023).

[9] *See* https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/#:~:text=The%20number%20of%20reported%20data%20breaches%20jumped%2068%20percent%20last,of%201%2C506%20set%20in%202017 (last accessed Jan. 10, 2023).

39. 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.

40. The ramifications of Five Guy's failure to keep its employee's PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue indefinitely.

41. 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 identity thieves. There are long-term consequences to data breach victims whose Social Security numbers are taken and used by identity thieves. Even if they know their Social Security numbers have been accessed, Plaintiff 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."

42. 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 were at risk and needed to be maintained safely and securely.

43. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgements of data security compromises, and despite

its own acknowledgement of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

Defendant, at all Relevant Times, had a Duty to Plaintiff and Class Members to Property Secure Their Private Information

44. At all relevant times, Defendant had a duty to Plaintiff 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 misuse, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, detect and prevent misuse of its systems and data by its own employees, and to *promptly* notify Plaintiff and Class Members when Defendant became aware that their PII may have been compromised.

45. 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 Plaintiff and Class Members.

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

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

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious or irregular use of its files;

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 unauthorized use of its servers;

h. Monitoring for unauthorized programs and websites being used by its employees;

i. Monitoring for unauthorized access and copying of sensitive PII;

j. Monitoring for suspicious or irregular server requests;

k. Monitoring for server requests for PII;

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

m. 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.

47. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[10] 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

48. The PII of individuals 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 credentials. For example, personal information can be sold at a price ranging from $40 to $200,

[10] 17 C.F.R. § 248.201 (2013).

and bank details have a price range of $50 to $200.[11] 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.[12]

49. 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.

50. 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.[13]

---

[11] *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 Jan. 10, 2023).

[12] *Dark Web Price Index 2021,* Zachary Ignoffo, March 8, 2021, *available at:* https://www.privacyaffairds.com/dark-web-price-index-2021/ (last accessed Dec. 20, 2022).

[13] Social Security Administration, *Identity theft and Your Social Security Number, available at:* https//www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 10, 2023).

51. 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.

52. 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]

53. 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.[15]

54. 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 identity thieves and cybercriminals in a variety of devastating ways. Indeed, the cybercriminal(s)/thieves who possess Plaintiff's and Class Members' PII can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

---

[14] 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 Jan. 10, 2023).

[15] 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 Jan. 10 , 2023).

55. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[16] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

56. To date, Defendant offered victims one year of credit monitoring and identity theft protection so long as they enroll by the March 29, 2023 deadline.[17] Plaintiff enrolled in this program. In offering such identity monitoring services Defendant recognized Plaintiff's and Class Members' need to protect their identities as a result of the Data Breach, yet, the offered services are inadequate to protect Plaintiff and Class Members from the threats they face presently and for years to come, particularly in light of the sensitive PII at issue here.

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

Defendant's Failure to Follow FTC Guidelines

58. 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.

---

[16] *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 Jan. 10, 2023).

[17] Notice of Security Incident filed with Maine Attorney General, file:///C:/Users/MICHA/Downloads/Five%20Guys_ME%20App%20&%20Sample%20(1).pdf (last visited on Jan. 10, 2023).

59. 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 security problems.[18] 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.[19]

60. 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.

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect personal data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

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

---

[18] 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 Jan. 10, 2023).
[19] *Id.*

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

64. Defendant was at all times fully aware of its obligation to protect the PII of its job applicants as well as past and present employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

65. 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.

66. 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.

67. 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.

68. 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

69. 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' PII;

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

d. Failing to properly monitor its own employees for the misuse of data;

e. Failing to implement and enforce its own data security policies to protect employees' PII;

f. Failing to train its employees in the proper handling of PII;

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

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

i. Failing to adhere to industry standards for cybersecurity.

70. As a result of the Data Breach, over 37,529 victims had their personal information stolen.

Harm to Employees

71. 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.

72. 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 a present and an increased risk of fraud and identity theft for many years into the future.

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

74. 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.

75. 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."[20]

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

77. 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.

78. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff 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 Plaintiff and Class Members as a result of a breach.

79. 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.

Plaintiff Lauren Turner's Experience

80. Plaintiff supplied PII to Five Guys in connection with a job application. She was an employee with Five Guys for in or around 2011.

81. On or around December 29, 2022, over a decade after working for Five Guys, Plaintiff Turner received a Notice of Data Breach, which stated her personal information, including her name and Social Security number, were impacted by the data breach.

[20] 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 Jan. 10 , 2023).

82. Plaintiff Turner has seen a marked increase in spam emails, texts, and phone calls since around the time of the September 2022 breach.

83. As a result of the Data Breach, Plaintiff's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff will have to worry about when and how her sensitive information may be shared or used to her detriment.

84. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

85. Additionally, Plaintiff is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

86. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

87. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

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

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

V. CLASS ALLEGATIONS

90. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiff brings this Action on behalf of herself and on behalf of all other persons similarly situated. Plaintiff proposes the following Class and Subclass definitions, subject to amendment as appropriate:

> All individuals residing in the United States whose PII was compromised in the data breach first announced by Defendant on or about December 29, 2022 (the "Class").
>
> All individuals residing in California whose PII was compromised in the data breach first announced by Defendant on or about December 29, 2022 (the "California Subclass").

91. Collectively the Class and California Subclass are referred to as the Classes.

92. 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.

93. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

94. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class wide relief because Plaintiff and all members of the Classes were subjected to the same wrongful practices by Defendants, entitling them to the same relief.

95. **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 Plaintiff at this time,

based on information and belief, the Class consists of over 100 individuals whose sensitive data was compromised in the Data Breach.

96. **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 Plaintiff's 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 Plaintiff 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 Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief;

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

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

99. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's 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 any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

100. **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.

101. 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

COUNT I

NEGLIGENCE
(On behalf of Plaintiff and the Class)

102. Plaintiff and the Class reallege and incorporate paragraphs 1-101 as if fully set forth herein. .

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

104. Five Guys required Plaintiff and Class Members to submit non-public Personally Identifiable Information, including but not limited to, Social Security Numbers, as a condition of employment at Five Guys .

105. Plaintiff 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.

106. By collecting and storing this data, and sharing it and using it for commercial gain, Five Guys 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.

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

108. 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 Plaintiff and Class Members, including harm that foreseeably could occur through the criminal acts of a third party.

109. Defendant owed a common law duty to Plaintiff 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 Plaintiff' s and Class Members' information in Defendant's possession was adequately secured and protected.

110. Defendant's common law duty it owed to Plaintiff 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.

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

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

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

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

115. Plaintiff 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 Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems.

116. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendant to take reasonable measures to protect Plaintiff's and the Class's PII and is a further source of Defendant's duty to Plaintiff 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.

117. 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 Plaintiff 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.

118. Defendant's own conduct created a foreseeable risk of harm to Plaintiff 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 Plaintiff's and the Class's PII, including basic encryption techniques available to Defendant.

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

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

121. Defendant owes Plaintiff and the Class a duty to adequately disclose that the PII of Plaintiff 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 Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

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

123. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiff 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 Plaintiff and the Class when the PII was within Defendant's possession or control.

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

125. 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.

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

127. 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.

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

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

130. There is a close causal connection between: (a) Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's 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.

131. As a direct and proximate result of Defendant's negligence, Plaintiff 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 Plaintiff's 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 Plaintiff and the Class Members.

132. Defendant breached the duties it owed Plaintiff 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.

133. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff 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.

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

135. 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.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

136. Plaintiff and the Class reallege and incorporate paragraphs 1-101 as if fully set forth herein

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

138. Five Guys solicited and invited prospective and current employees to provide their PII as part of its regular business practices. These individuals accepted Five Guys's offers and provided their Information to Five Guys. In entering into such implied contracts, Plaintiffs and the Class reasonably presumed that Five Guys's data security practices and policies were reasonable

and consistent with industry standards, and that Five Guys would use part of the funds received from Plaintiff's and the Class's labor to pay for adequate and reasonable data security practices.

139. Plaintiff and the Class would not have provided and entrusted their Information to Five Guys in the absence of the implied contract between them and Five Guys to keep the information secure.

140. Plaintiff and the Class fully performed their obligations under the implied contracts with Five Guys .

141. Five Guys breached its implied contracts with Plaintiff 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.

142. As a direct and proximate result of Five Guys's breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

143. Plaintiff and the Class reallege and incorporate paragraphs 1-101 as if fully set forth herein.

144. Plaintiff brings this count on behalf of themselves and the Class in the alternative to the other Counts alleged herein to the extent necessary.

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

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

147. The money that Defendant received from Plaintiff's 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 Plaintiff's and Class Members' PII.

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

149. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff 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 Plaintiff's PII.

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

151. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiff's and Class Members' PII, Plaintiff 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.

152. 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 Plaintiff and the Class.

153. 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 Plaintiff and the Class for restitution in the amount of the benefit conferred on Defendant as a result of its wrongful conduct.

COUNT IV
CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
Cal. Civ. Code § 1798.100, *et seq.*

(On behalf of Plaintiff and the California Subclass)

154. Plaintiff and the Class reallege and incorporate paragraphs 1-102 as if fully set forth herein.

155. This Count is brought on behalf of Plaintiff and the California Subclass against Defendant.

156. Defendants violated sections 1798.81.5(b) and 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiff's and the California Subclass' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

157. The non-redacted and non-encrypted PII of Plaintiff and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendants' violations of their duty under the CCPA.

158. Plaintiff and the California Subclass lost money or property, including but not limited to, the loss of legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as a direct and proximate result of Defendants' acts described above.

159. Defendant knew, or should have known, that their network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the PII so in the event of a data breach an unauthorized third party cannot read the PII. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiff and members of the California Subclass was exposed.

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

161. Defendant is organized for the profit or financial benefit of their owners and collect PII as defined in Cal. Civ. Code § 1798.

162. Plaintiff and the Class Members 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."

163. Plaintiff and the California Subclass seek injunctive or other equitable relief to ensure that Defendants hereinafter adequately safeguard PII by implementing reasonable security procedures and practices. This relief is important because Defendant still holds PII related to Plaintiff and the California Subclass. Plaintiff and the California Subclass have an interest in ensuring that their PII is reasonably protected.

164. Pursuant to § 1798.150(b) of the CCPA, Plaintiff gave written notice to Defendant of their specific violations of sections 1798.81.5(b) and 1798.150(a) by email to outside counsel, by agreement, on January 11, 2023. If Defendant does not "actually cure" the effects of the Data Breach, which would require, at minimum, retrieving the PII or securing the PII from continuing and future use, within 30 days of delivery of the CCPA notice letter (which Plaintiff believes any such cure is not possible under these facts and circumstances), Plaintiff intends to amend this complaint to seek actual damages, or statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach, on behalf of the California Subclass.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff 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 Plaintiff and

Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

C. For equitable relief compelling Defendant to use appropriate methods and policies with respect to 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 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 PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII 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 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 and identity theft protection services for Plaintiff 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 Plaintiff and members of the putative Class.

DATED: January 11, 2023 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

Scott M. Perry, VSB #67417
BREIT BINIAZAN, P.C.
1010 N. Glebe Road, Suite 310
Arlington, Virginia 22201
Telephone: (703) 291-6666
Facsimile: (703) 563-6692
Scott@bbtrial.com

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

ClassAction.org
