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

ERIKA RANCK, on behalf of herself and all others similarly situated, Plaintiff, v. FIVE GUYS ENTERPRISES, LLC, Defendant.	Case No. 1:23-cv-34 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Erika Ranck, through her attorneys, brings this Class Action Complaint against the Defendant, Five Guys Enterprises, LLC ("Five Guys" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, alleging as follows:

INTRODUCTION

1. Five Guys operates 1,700 hamburger restaurants worldwide, employing thousands of people. 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"), exposing all of its current, former, and prospective employees to a lifelong risk of identity theft and fraud.

2. Plaintiff brings this class action against Five Guys for its failure to properly secure and safeguard her personally identifiable information ("PII"), which includes *at least* her name and Social Security number.

3. Five Guys requests, collects, and maintains the PII of Plaintiff and members of the Classes, all of whom are current, former, and prospective employees. Five Guys stored this

PII unencrypted and in an Internet-accessible environment on Defendant's network.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and members of the Classes, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. Indeed, Five Guys claims to "understand[] the importance of protecting the information that [it] maintain[s]."[1]

6. Despite this understanding, Five Guys failed to implement reasonable security measures to protect Plaintiff's and Class members' PII, allowing an unknown actor to access its network, including files that contained the PII of Plaintiff and members of the Classes.

7. Yet, despite Five Guys learning of the Data Breach on September 17, 2022, Five Guys did not begin notifying Plaintiff and members of the Classes until December 29, 2022, that their PII had been compromised.

8. In its Breach Notice, Five Guys admits that its inadequate security systems were bypassed and the files that were accessed included information submitted to Five Guys in connection with the employment process, including name and Social Security numbers, *at a minimum*.

9. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its prospective, current, and former employees how many people were impacted, how the breach happened (i.e., what the specific security vulnerabilities and root causes were), or why it took the Defendant over three months to begin notifying victims that hackers had gained access to highly sensitive employee information.

10. Defendant's failure to timely detect and report the Data Breach made its current

[1] December 29, 2022 Breach Notice from Five Guys. Attached as **Exhibit A**. ("Breach Notice").

and former employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII, all while criminals were misusing the PII.

11. Exposing this information devastates breach victims. Not only has the breach exposed their PII, they now face a lifelong risk of identity theft because the breach divulged information they cannot change, like their Social Security numbers.

12. Indeed, after the Data Breach, Ms. Ranck suffered repeated fraud and identity theft. Had Five Guys notified her about the breach "without unreasonable delay" as Virginia law requires, she could have prevented or mitigated that harm.

13. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

14. In its Breach Notice, Five Guys recognizes how its breach threatens its current, former, and prospective employees, as it is warning them to monitor their accounts for fraud, freeze their credit accounts, sign up for credit monitoring, and report any fraud to their providers. As a result, Plaintiff and members of the Classes are not only suffering harm from the Data Breach, but must spend time and resources to mitigate the harm it will cause in the future.

15. Ms. Ranck is a Data Breach victim. She brings this Class Action on behalf of herself and all others harmed by Defendant's misconduct.

16. Defendant disregarded the rights of Plaintiff and members of the Classes by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and members of the Classes was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and

failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and members of the Classes was compromised through disclosure to an unauthorized third party. Plaintiff and members of the Classes have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

17. Plaintiff and members of the Classes 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.

PARTIES

18. Plaintiff Erika Ranck is a natural person and citizen of Virginia, where she intends to remain. Ms. Ranck is a Data Breach victim, receiving Defendant's Breach Notice on or around January 3, 2023.

19. Defendant Five Guys is a Virginia corporation with a principal place of business in Lorton, Virginia.

JURISDICTION & VENUE

20. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or

value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed classes, and at least one member of the Nationwide Class is a citizen of a state different from Defendant.

21. This Court has personal jurisdiction over Defendant because its principal place of business is located in this District and the events related to this action arose out of this District.

22. Venue is proper because Defendant's principal place of business is located in this District.

BACKGROUND FACTS

A. Five Guys

23. Five Guys requested and collected the PII of Plaintiff and members of the Classes, who include prospective employees who have submitted job applications containing their PII, and current and former employees.

24. On information and belief, the PII Five Guys collected includes, at least, names, Social Security numbers, dates of birth, and financial account and routing numbers for those employees receiving compensation through direct deposit.

25. Five Guys maintains the PII of former employees and job applicants for years, many years after the application was submitted and rejected or the employee was terminated.

26. Five Guys had a duty to adopt reasonable measures to protect Plaintiff's and Class members' PII from involuntary disclosure to third parties.

27. In collecting and maintaining the PII, Five Guys implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

28. Plaintiff and members of the Classes trusted Five Guys to keep their PII confidential and securely maintained, to use this information to hire and administer their employment, and to only make authorized disclosures of this information pursuant to state and

federal laws.

29. Plaintiff would not have entrusted her PII to Five Guys had she known it would fail to securely protect and maintain her PII.

30. Employees place value in data privacy and security. These are important considerations when deciding who to work and provide services for. Plaintiff would not have accepted the Defendant's employment offer, nor provided her PII, to Five Guys had she known that Five Guys does not take all necessary precautions to secure the personal and financial data given to it by its employees.

B. Five Guys Fails to Safeguard Employment PII

31. Defendant's security lapses arose from how it stores its prospective, current, and former employees' employment information.

32. Despite its duties and alleged commitments to safeguard PII, Five Guys does not follow industry standard practices in securing employees' PII.

33. Five Guys, on information and belief, has not implemented reasonable cybersecurity safeguards or policies to protect employment PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Five Guys leaves vulnerabilities in its systems for cybercriminals to exploit and gain access to PII contained within employment information.

34. Because Five Guys failed to implement these and other safeguards to protect its system from a hack, criminals could access the system and steal the records belonging to Plaintiff and members of the Classes.

35. Because of these failures, according to the Breach Notice, on September 17, 2022, Five Guys realized that an unknown third party had unauthorized and unrestricted access to files on its system for an unknown amount of time, and that these "files contained information

submitted to Five Guys in connection with the employment process." Exhibit A.

36. Five Guys was unable to detect the presence of cybercriminals in its systems before criminals could access or remove the files containing PII in employment information from its systems.

37. On information and belief, Five Guys failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over employment PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. Further, the Breach Notice makes clear that Five Guys cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

38. After the Data Breach, Five Guys "immediately" implemented its incident response plan, launched an investigation, notified law enforcement, but failed to also immediately notify those whose PII had been accessed.

39. It took Five Guys at least three months to notify the Data Breach victims, including Plaintiff and members of the Classes.

40. As a result, Plaintiff and members of the Classes had no reason to guard themselves against identity theft and fraud following the hack.

41. For several months, Ms. Ranck has experienced fraudulent charges in her name at both U-Haul and Walmart. Before Five Guys announced the breach, she had no idea what initiated the rampant fraud affecting her personal accounts.

42. As early as December 29, 2022, Five Guys finally disclosed its breach to its current, former, and prospective employees. In its Breach Notice, Five Guys advised that victims "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free

credit reports for any unauthorized activity."

43. Most concerning, Five Guys states in its Breach Notice that, "[t]o prevent something like this from happening again, [it has] taken steps to enhance [its] existing security measures." Not only should these measures have been in place *before* the Data Breach, Five Guys fails to say specifically what these measures are which is important because Five Guys still maintains Plaintiff's and Class members' PII.

44. Five Guys has offered only one year of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers. Further, the breach exposed employees' nonpublic financial information, a disturbing harm in and of itself.

45. Even with complimentary credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

46. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class members' PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class members' financial accounts.

C. Plaintiff's Experience

47. Ms. Ranck is a Data Breach victim, receiving Defendant's Breach Notice in early January 2023.

48. Ten years ago, Ms. Ranck was employed by Five Guys for 2-3 months.

49. Ms. Ranck does not recall ever learning that her information was compromised in

a data breach incident, other than the breach at issue in this case.

50. When she was seeking employment with Five Guys, Five Guys requested she provide her PII as a condition of her employment.

51. Ms. Ranck trusted Five Guys would use reasonable measures to protect her PII according to Defendant's internal policies, as well as state and federal law. She complied with its request and provided her PII to Five Guys. Indeed, she viewed reasonable data protection as implicit in her agreement to provide her PII to Five Guys in return for paid employment.

52. Ms. Ranck received a Breach Notice on January 3, 2023, indicating that her PII, including at least her name and Social Security number, was compromised in the Data Breach. In addition to the damages detailed herein, the Data Breach has caused Ms. Ranck to be at a substantial risk for further identity theft.

53. In fact, because Five Guys failed in its duties, Ms. Ranck has suffered repeated fraud. Her name and credit are being used to open multiple accounts.

54. On January 5, 2023, Ms. Ranck received an email from U-Haul's collections department stating she owes U-Haul $118.05 from a reservation made on December 2, 2022 fraudulently made in her name. Ms. Ranck did not make any reservation with U-Haul in December 2022.

55. Additionally, for the last several months, Ms. Ranck has received notifications from a Walmart+ account fraudulently associated with her phone number, name, email address, and home address.

56. As a result of the Data Breach and the recommendations of Defendant's Breach Notice, Ms. Ranck made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account

statements, changing her online account passwords, and monitoring her credit information as suggested by Five Guys.

57. Ms. Ranck has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. In fact, she has devoted over two full workdays to addressing the ramifications of the Data Breach. Ms. Ranck fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Ms. Ranck has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

58. Ms. Ranck is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing its current, former, and prospective employees about the Data Breach.

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

D. Plaintiff and the Proposed Classes Face Significant Risk of Continued Identity Theft

60. Plaintiff and members of the proposed Classes have suffered injury from the misuse of their PII that can be directly traced to Defendant.

61. The ramifications of Defendant's failure to keep Plaintiff's and the Class members' PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, or other nonpublic financial information, without permission, to commit fraud or other crimes.

62. The types of personal data compromised and potentially stolen in the Five Guys Data Breach is highly valuable to identity thieves. The employees' stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

63. Identity thieves can also use this data to harm Plaintiff and members of the Classes through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health- related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

64. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Classes have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

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

66. The value of Plaintiff's and Class members' PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

67. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

68. One such example of criminals using PII for profit is the development of "Fullz" packages.

69. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

70. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and members of the proposed Classes' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Classes, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Classes' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

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

72. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed

the PII of Plaintiff and members of the proposed Classes to unscrupulous operators, con artists, and criminals.

73. Defendant's failure to properly notify Plaintiff and members of the proposed Classes of the Data Breach exacerbated Plaintiff and members of the proposed Classes' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

E. Five Guys Failed to Adhere to FTC Guidelines.

74. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

75. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

76. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

77. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

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

F. Plaintiff and members of the Classes Suffered Damages

80. The compromised and stolen PII of Plaintiff and members of the Classes is private and sensitive in nature and was left inadequately protected by Acts. Defendant did not obtain Plaintiff's and Class members' consent to disclose this data to any other person as required by applicable law and industry standards.

81. As discussed above, Plaintiff's personal, private, and sensitive data, including but not limited to financial data, which Five Guys allowed to be stolen has already been used to inflict harm on Plaintiffs.

82. Plaintiff has experienced multiple instances of fraud.

83. The data breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class members' personal data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including the failure to establish and implement appropriate

administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' sensitive personal information to protect against reasonably foreseeable threats to the security or integrity of such information.

84. Had Five Guys remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Five Guys would have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and the Class Members' confidential personal, sensitive, and private information and data.

85. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting data breach, Plaintiff and members of the Classes have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

86. Defendant's wrongful actions and inaction directly and proximately caused the potential theft and dissemination into the public domain of Plaintiff's and Class members' personal data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

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

c. the actual, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class members' information on the Internet's black market;

d. the untimely and inadequate notification of the data breach;

e. the improper disclosure of their personal data;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

h. ascertainable losses in the form of deprivation of the value of their personal data, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the data breach;

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

k. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of

withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data breach.

G. Defendant's Offer of Credit Monitoring is Inadequate

87. At present, Five Guys has offered one year of free credit monitoring provided by IDX to breach victims.

88. As previously alleged, Plaintiff's and the Class members' personal data may exist on the Dark Web and in the public domain for months, or even years, before it is used for ill gains and actions. With only one year of monitoring, Plaintiff and members of the Classes remain unprotected from the real and long-term threats against their personal, sensitive, and private data.

89. Therefore, the "monitoring" services offered by Five Guys are inadequate, and Plaintiff and members of the Classes have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

CLASS ACTION ALLEGATIONS

90. Plaintiff sues on behalf of herself and the proposed Nationwide Class, defined as follows:

> All individuals residing in the United States whose PII was compromised in the Data Breach disclosed by Five Guys in December 2022.

91. Plaintiff sues on behalf of herself and the proposed Virginia Class, defined as follows:

> All Virginia residents whose PII was compromised in the Data Breach disclosed by Five Guys in December 2022 and received notice after an unreasonable delay.

92. Excluded from the Classes are Defendant, its agents, affiliates, parents,

subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

93. Plaintiff reserves the right to amend the definitions of either Class.

94. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the proposed Classes, consisting of 2.2 million members, far too many to join in a single action;

b. **Ascertainability**. Members of the Classes are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Classes' interests. Their interests do not conflict with Class members' interests and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Classes' behalf, including as lead counsel.

e. **Commonality**. Plaintiff and the Classes' claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all members of the Classes. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class members' PII;

ii. 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;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class members' PII;

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

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class members' injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and members of the Classes are entitled to damages, treble damages, or injunctive relief.

95. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

96. Plaintiff reallege all previous paragraphs as if fully set forth below.

97. Plaintiff and members of the Class entrusted their PII to Five Guys. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting

their personal data and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the personal data of Plaintiff's and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

98. Five Guys was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class members' sensitive data on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

99. Defendant knew that the personal data of Plaintiff and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the personal data of Plaintiff and the Class was wrongfully disclosed, that disclosure was not fixed.

100. By being entrusted by Plaintiff and the Class to safeguard their personal data, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their personal data with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

101. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was requested, stored, used, and exchanged, and those in its employ who were responsible for making that happen. Indeed, Defendant actively sought and obtained Plaintiff's and members of the Class's PII.

102. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' personal data by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiff's and the other Class member's personal data.

103. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their personal data would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the personal data of Plaintiff and the Class and all resulting damages.

104. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' personal data. Defendant knew its systems and technologies for processing and securing the personal data of Plaintiff and the Class had numerous security vulnerabilities.

105. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

106. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face. Plaintiff and the Class have also suffered increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

107. Plaintiff and the Class have also suffered consequential out of pocket losses for

procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Class)

108. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

109. Plaintiff alleges this negligence *per se* theory as alternative to her other negligence claims.

110. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

111. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customer information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

112. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

113. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein.

114. Defendant's violation of Section 5 of the FTC Act and its failure to comply with

applicable laws and regulations constitutes negligence *per se*.

115. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

116. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

117. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

118. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

119. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

120. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores

and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

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

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

122. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

123. Five Guys required Plaintiff and Class members to provide their PII as a condition of obtaining employment with Five Guys.

124. As part of the process of seeking employment with Five Guys, Plaintiff and Class members provided and entrusted their PII to Five Guys.

125. By entrusting their PII to Five Guys. Plaintiff and Class members provided something of value to Five Guys, regardless of whether their application for employment was accepted. Five Guys received the benefit of the PII and was given a potential employee. Consideration was exchanged, regardless of whether the application for employment was accepted. Moreover, Five Guys retained the PII from rejected applications, showing the value that PII had to Five Guys (otherwise it would have just deleted the PII).

126. Five Guys solicited potential employees' PII as a pre-condition for considering whether to provide employment to that person; it then continued to possess and aggregate that

PII with other current, former, and prospective employees' PII for its own business purposes, beyond those pertaining to the particular employee whose PII was obtained.

127. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect their PII, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

128. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

129. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such agreement.

130. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant by providing the PII to Five Guys and/or performing employment obligations, or such performance was waived by the conduct of Defendant in rejecting their application.

131. Defendant materially breached the contract(s) it entered with Plaintiff and members of the Class by failing to safeguard and protect their PII, by failing to delete the information of Plaintiff and the Class once the relationship ended, and failing to accurately and timely notify them of the intrusion into its computer systems that compromised their PII.

132. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are

necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

133. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

134. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

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

136. Subterfuge and evasion violate the obligation of good faith in performance even

when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

137. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

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

139. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT VI
VIRGINIA DATA BREACH NOTIFICATION LAW
Virginia Code §§ 18.2-186.6(B)
(On Behalf of Plaintiff and the Virginia Subclass)

140. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

141. Virginia Code § 18.2-186.6(B) requires entities that possess the computerized data of a Virginia resident, including personal information, must disclose without unreasonable delay any breach of its security system upon discovery or notification of the breach. Notice must go to the Office of the Attorney General and any affected Virginia resident.

142. This statute applies to Five Guys because it "maintains computerized data that includes personal information that the individual or entity does not own or license," pursuant to Virginia Code § 18.2-186.6(D).

143. This statute expressly authorizes a Virginia resident to recover direct economic damages.

144. Virginia Code § 18.2-186.6(A) defines "personal information" as "the first name or first initial and last name in combination with and linked to any one or more of the following

data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number."

145. Plaintiff's personal information, as defined by Virginia Code § 18.2-186.6(A), including her name and Social Security number, was compromised in the Data Breach.

146. Defendant's Breach Notice was sent at least three months after Five Guy's discovered the Data Breach. This Breach Notice was not timely sent and constitutes unreasonable delay.

147. Plaintiff has suffered economic injury due to and traceable from the timing of the delayed notification. First, her economic injuries are solely the result of the Data Breach itself. Second, if she had been aware of the Data Breach earlier, she could have taken additional steps to prevent the identity theft that came to pass and the economic injuries arising therefrom.

COUNT V
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class)

148. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

149. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

150. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and the Nationwide Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and the Nationwide Class from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and remains at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

151. Plaintiff and the Classes have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiff's and the Nationwide Class's PII, including Social Security numbers, while storing it in an Internet-accessible environment and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security number of Plaintiff.

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

a. Defendant owes a legal duty to secure the PII of Plaintiff and the Nationwide Class;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiff harm.

153. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and

government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards;

d. implement an education and training program for appropriate employees regarding cybersecurity.

154. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

155. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

156. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and others whose

confidential information would be further compromised

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

157. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

158. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

159. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of disclosing their PII.

160. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff and members of the Class's PII, as this was used to facilitate employment by Defendant.

161. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of the benefits Plaintiff and the Class conferred because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII had they known Defendant would not adequately protect their PII.

162. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

Plaintiff and members of the Classes demand a jury trial on all claims so triable and request that the Court enter an order:

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

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Classes;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Classes;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Classes damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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

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

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

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 10th day of January, 2023.

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

Samuel J. Strauss*
Raina Borrelli*
TURKE & STRAUSS, LLP
613 Williamson Street #201
Madison, WI 53703
Tel: (608) 237-1775
Sam@turkestrauss.com
Raina@turkestrauss.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Tel.: 866.252.0878
gklinger@milberg.com

**pro hac vice forthcoming*

Attorneys for Plaintiff