IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

JOSEPH LIPTOCK, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. MASTEC, INC., Defendant.	Case No. 2:23-cv-5753-MDL **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Joseph Liptock ("Plaintiff") brings this action on behalf of himself, and all others similarly situated, against Defendant MasTec, Inc. ("Defendant" or "MasTec"). Plaintiff seeks to obtain damages, restitution, and injunctive relief for a putative class of individuals who are similarly situated employees of Defendant (the "Class"). Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of a MOVEit-related data breach at Delta Dental which affected employees and dependents enrolled in the company's Care Opt Plus Group Benefits Plan For Hourly & Salaried Employees.[1]

2. Delta Dental Plans Association is the self-proclaimed nation's leading provider of dental

[1] https://www.jdsupra.com/legalnews/mastec-employees-may-be-the-victim-of-9686189/ (last accessed November 9, 2023).

insurance.[2] Delta Dental is a not-for-profit organization that serves more than 80 million Americans.[3]

3. MOVEit is a file transfer platform made by Progress Software Corporation. The platform is used by thousands of governments, financial institutions and other public and private sector bodies all around the world to send and receive information.[4]

4. In late May 2023, data started to be transferred from hundreds of MOVEit deployments, however, these were not normal file transfers initiated by legitimate users. MOVEit had been hacked and the data was being stolen by a ransomware operation called Cl0p.[5]

5. The current tally of organizations and individuals known to have been impacted by this incident is 2,569. The data is sourced from state breach notifications, SEC filings, other public disclosures, as well as Cl0p's website, and is current as of November 9, 2023.[6]

6. In sum, Defendant is an employer who offers health related benefits to its employees. To receive these benefits, Plaintiff and other employees were required to provide information. Unfortunately, such information provided to Defendant was not properly secured.[7]

7. The cyberattack resulted in a breach of Defendant's employees' documents and information ("The Data Breach").[8] The documents and information include, but are not limited to: employee names, social security numbers, date of birth, gender, member contact information, member IDs, eligibility dates, and provider information. ("Personal Identifiable Information" or

---

[2] https://www.deltadental.com/us/en/about-us.html#:~:text=Who%20we%20are,not%2Dfor%2Dprofit%20organization.
[3] *Id.*
[4] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/ (Last accessed November 9, 2023).
[5] *Id.*
[6] *Id.*
[7] https://www.jdsupra.com/legalnews/mastec-employees-may-be-the-victim-of-9686189/ (last accessed November 9, 2023).
[8] *Id.*

"PII"). [9]

PARTIES

8. Plaintiff Joshua Liptock is an individual citizen of the State of South Carolina, residing in the city of Summerville, which is located within Berkeley County.

9. Plaintiff is a former employee of Defendant. Plaintiff worked for Defendant from 2021 to around September of 2023.

10. Defendant MasTec is a for profit corporation, organized and incorporated under the laws of Florida and headquartered in Coral Gables, Florida.

11. Defendant is a civil engineering and construction company that provides engineering, building, installation, maintenance, and upgrade services for communications, energy, utility, and other infrastructure sector customers in the United States, Canada, and abroad.[10]

12. Defendant's principal place of business is located at 800 S. Douglas Road, 10th Floor, Coral Gables, FL 33134.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more putative Class Members, (ii) the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest and costs, and (iii) there is minimal diversity because Plaintiff and Defendant are citizens of different states.

14. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367.

15. This Court has personal jurisdiction over Defendant because it has substantial aggregate

[9] *Id.*
[10] *Id.*

contacts with this District, including engaging in conduct in this District that has a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, and because it purposely availed itself of the laws of the United States and South Carolina, including in this District, is registered to do business in this jurisdiction, and/or has caused its products/services to be disseminated in this District.

16. Venue in this district is proper in this Court pursuant to 28 U.S.C. §1391 because Plaintiff resides in this District, a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District, Defendant transacts business in this District, and has intentionally availed itself of the laws and markets within this District.

FACTUAL ALLEGATIONS

17. The Data Breach occurred roughly 5 months ago in May of 2023, around May 27th and continuing to roughly May 30th.[11] Defendant allowed Plaintiff and the Class's data to be breached for three continuous days.

18. Sadly, Plaintiff and other employees of Defendant were not given such notice of the breach until on or around October 27th, 2023.[12] 153 days passed between Defendant being hacked and Defendant letting Plaintiff know of his breach.[13] 153 days is plenty of time for a hacker to use Plaintiff's information, in fact, many files are often accessed by bad actors within 12 hours of a breach.[14]

19. As a result of this cyberattack, Plaintiff and other employees of Defendant who have had their data breached and disseminated have suffered and will continue to suffer as their PII has been

[11] *See* Plaintiff's Notice to Impacted Individuals, dated October 27, 2023, attached as **Exhibit A.**
[12] *Id*.
[13] https://www.timeanddate.com/date/durationresult.html?m1=5&d1=27&y1=2023&m2=10&d2=27&y2=2023&ti=on
[14] https://ksltv.com/468945/how-quickly-hackers-access-use-your-personal-data-following-a-data-breach/ (last accessed November 9, 2023).

leaked and will continue to be on the internet for the foreseeable future.

20. Upon information and belief, the data that was breached is related to current and former employees of Defendant, which includes nearly twenty-two thousand individuals, including Plaintiff.[15]

21. Defendant is a civil engineering and construction company based out of Coral Gables, Florida. Defendant provides engineering, building, installation, maintenance, and upgrade services for communications, energy, utility, and other infrastructure sector customers in the United States, Canada, and abroad.[16]

22. Defendant holds and stores certain highly sensitive PII of the Plaintiff and the Class Members on its computer network. This includes individuals who are current or former employees of Defendant itself. The Plaintiff and accompanying Class includes (but may not be limited to) individuals who provided their extremely sensitive and personal, private information to be considered for employment purposes and benefits.

23. Further, in regard to itself, Defendant states: "With offices across North America, a workforce of nearly 22,000 skilled professionals and an extensive wholly-owned fleet of specialized construction equipment, MasTec has the resources needed to handle even the most complicated jobs."[17]

24. Unfortunately, despite tens of thousands of skilled professionals and specialized equipment, Defendant did not have the resources to handle the straightforward and obviously needed job of safeguarding Plaintiff's PII.

25. Defendant was required to begin notifying victims of its Data Breach as soon as possible,

[15] https://www.mastec.com/about/
[16] https://www.jdsupra.com/legalnews/mastec-employees-may-be-the-victim-of-9686189/
[17] *Id.*

informing them that their PII had been stolen in a data breach affecting an unknown number of individuals, but this number may harm all 22,000 or more of Defendant's employees. Defendant waited 153 days to notify Plaintiff and the Class.

26. In its Notice to Impacted Individuals Letter to Plaintiff, Defendant admitted: "Delta Dental indicated that certain data stored in Delta Dental's MOVEit application was downloaded by an unauthorized actor between May 27 and May 30, 2023. When Delta Dental became aware of this incident, Delta Dental promptly took the affected application offline and updated systems to secure vulnerabilities and prevent further access. Outside advisors and cybersecurity experts were retained to assist in the evaluation of the situation. On July 21, 2023, we learned that certain Plan member data may have been impacted in Delta Dental's incident."[18]

27. Further, Defendant stated: "On August 15, 2023, we completed our investigation and confirmed that some of your personal information was impacted."[19]

28. In sum, Defendant passes the buck to its chosen medical providers and servicers, Delta Dental and MOVEit. Rather than showing accountability and Defendant devoted time and resources to this breach only reactively, rather than proactively.

29. As a result of Defendant's Data Breach, Plaintiff and thousands of Class Members suffered ascertainable losses in the form of financial losses resulting from identity theft, out-of-pocket expenses, the loss of the benefit of their bargain, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

30. Plaintiff's extremely sensitive PII, entrusted to Defendant was compromised, intentionally accessed, and removed by the cyber-criminals who perpetrated this attack, where it remains in the hands of those cyber-criminals.

[18] *See* Plaintiff's Notice to Impacted Individuals, dated October 27, 2023, attached as **Exhibit A.**
[19] *Id.*

31. Defendant offered two years of credit monitoring through Experian.[20] But this offer is insufficient as to adequately protect Plaintiff.

32. This above offer does not protect Plaintiff fully from Defendant's Breach. PII does not go away and remains on the internet forever.

33. Plaintiff and the Class would have to all change their social security numbers and addresses to combat the Breach, even remotely. Given the nearly six-month delay in even disclosing the Breach, and a two year offer to protect permanently leaked information, it is clear to see that Defendant does not truly care about its employees.

34. The fact remains that Plaintiff's Information was not properly, seriously, and adequately safeguarded when Defendant was breached.

35. Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's Private Information directly resulted in the Data Breach.

36. Plaintiff brings this class action on behalf of himself and other similarly situated job applicants, current or former employees, or other individuals who received a Notice to Impacted Individuals Letter from Defendant or its affiliates.

37. Plaintiff seeks to address the grossly inadequate safeguarding of the PII that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff that his PII had been accessed and acquired by an unknown third party. Defendant also failed to identify precisely what PII was accessed that belonged to Plaintiff.[21]

38. Defendant preserved the PII in a reckless manner; particularly, the PII was kept on Defendant's computer network in a condition vulnerable to cyberattacks, including the ransomware attack that occurred. Because the mechanism of the cyberattack and potential for

[20] *Id*.
[21] *Id.*

improper disclosure of Plaintiff's PII was a known risk to Defendant, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

39. Defendant disregarded the privacy and property rights of Plaintiff by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data and computer systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff prompt and accurate and complete notice of the Data Breach.

40. Had Defendant not failed to properly monitor the computer network and systems that housed the PII, it would have discovered the intrusion promptly, and potentially been able to stop the intrusion or, at the very least, mitigate the injuries to the Plaintiff.

41. Plaintiff and other Class Members' identities are now at substantial and imminent risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained (including Social Security numbers) is now in the hands of cybercriminals.

42. Using the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, *inter alia*, opening new financial accounts or taking out loans in Plaintiff's name, using Plaintiff's information to receive government benefits, filing fraudulent tax returns, filing false medical claims using Plaintiff's information, obtaining driver's licenses in Plaintiff's name but with another person's photograph, and giving false information to police during an arrest.

43. Plaintiff is suffering from fraudulent activities or has been exposed to a heightened risk of fraud and identity theft due to Defendant's data breach. Plaintiff must now (and for years into the future) closely monitor his personal and financial accounts to guard against identity theft.

44. Plaintiff will likely incur out of pocket costs for, *e.g.*, unreimbursed fraudulent charges, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

45. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach and, as such, brings this action against Defendant for negligence, breach of implied contract, unjust enrichment, and declaratory relief, seeking redress for Defendant's unlawful and reckless conduct.

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

47. As well discussed above, on May 27, 2023, Defendant experienced a Data Breach. On October 27, 2023, Defendant reported this data breach to the Montana Attorney General.[22] On that same day, Defendant finally made Plaintiff aware that the breach harmed him.

48. Plaintiff's "Notice to Impacted Individuals" Letter is dated October 27, 2023, and Defendant's model letter provided to the Montana AG is dated October 27, 2023. Thus, ***Plaintiff's PII was in the hands of cybercriminals for at least 5 months before he was notified*** of the Data Breach. Early notification is critical when trying to protect against identity theft after a data breach.

49. Upon information and belief, the cyberattack was targeted at Defendant as a large employer that collects and maintains valuable personal and financial data from its current and former employees and applicants.

50. Upon information and belief, the PII stored on Defendant's network was not encrypted.

[22] https://www.jdsupra.com/legalnews/mastec-employees-may-be-the-victim-of-9686189/

51. Plaintiff's PII was accessed and stolen in the Data Breach. Plaintiff reasonably believes his stolen PII is currently available for sale, or was already subsequently sold, on the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that collect PII.

52. Defendant had obligations created by contract, industry standards, and common law to keep Plaintiff's PII confidential and to protect it from unauthorized access and disclosure.

53. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

Acquiring, Collecting, and Storing PII and Preventing Breaches

54. Defendant, as part and parcel of offering healthcare benefits to its employees, acquires, collects, and stores a massive amount of PII of individuals who are employed or seeking employment through it or its franchisees or subsidiaries.

55. By obtaining, collecting, and using Plaintiff's PII for its own financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiff's PII from disclosure.

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

57. Plaintiff has taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep his PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Ransomware Attack and the Data Breach were Foreseeable Risks of which Defendant was on Notice

58. It is well known that PII, including Social Security numbers, is a valuable commodity and a frequent, intentional target of cyber criminals and hackers. Companies that collect such information, including Defendant, are well aware of the risk of being targeted by cybercriminals.

59. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes "significant negative financial impact on victims," severe negative repercussions to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

60. Data Breach victims suffer long-term and, sometimes, lifelong consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff cannot obtain new numbers unless he has become a victim of social security number misuse.

61. 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.[23]

62. In light of 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), Estee 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 computer network would be targeted by cybercriminals.

63. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued

[23] https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed November 7, 2023).

a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

64. According to an FBI publication, "Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data."[24]

65. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs from being compromised.

Defendant Had a Duty to Plaintiff to Properly Secure his PII

66. At all relevant times, Defendant had a duty to Plaintiff to properly secure his PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff, and to *promptly* notify Plaintiff when Defendant became aware that his PII was compromised.

67. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff. The special relationship arose because Plaintiff entrusted Defendant with their PII when they were employees or merely job applicants.

68. 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.

[24] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed November 7, 2023).

69. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

- Maintaining a secure firewall configuration;
- Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
- Monitoring for suspicious or irregular traffic to servers;
- Monitoring for suspicious credentials used to access servers;
- Monitoring for suspicious or irregular activity by known users;
- Monitoring for suspicious or unknown users;
- Monitoring for suspicious or irregular server requests;
- Monitoring for server requests for PII;
- Monitoring for server requests from VPNs; and
- Monitoring for server requests from Tor exit nodes.

70. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[25] 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."[26]

71. The ramifications of Defendant's failure to keep consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent

[25] 17 C.F.R. § 248.201 (2013).
[26] *Id.*

use of that information and damage to victims including Plaintiff may continue for years.

The Value of Personal Identifiable Information ("PII").

72. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[27]

73. 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 uses 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:

> 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, 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.[28]

74. It is extremely difficult 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. 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.

75. Even a new Social Security number may not be effective, as "[t]he credit bureaus and

---

[27] *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 November 7, 2023).

[28] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed November 7, 2023).

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."[29]

76. As one would expect, this data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[30]

77. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver's licenses, government benefits, medical services, and housing, give false information to police, and obtain tax returns or open fraudulent credit card accounts in Plaintiff's names.

78. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

79. Defendant's credit monitoring offer and advice to Plaintiff places the burden on Plaintiff, rather than the Defendant, to monitor and report suspicious activities to law enforcement. Defendant expects Plaintiff to protect himself from *Defendant's* tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff about actions he can affirmatively take to protect himself.

80. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing

[29] Bryan 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 accessed November 7, 2023).
[30] 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-credit-card-numbers.html (last accessed November 7, 2023).

identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's PII.

81. The injuries to Plaintiff were directly and proximately caused by Defendant' failure to implement or maintain adequate data security measures for the victims of its Data Breach.

Defendant Failed to Comply with FTC Guidelines.

82. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

83. 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.[32] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as 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 security problems.

84. The FTC recommends that businesses:

- Identify all connections to the computers where you store sensitive information.
- Assess the vulnerability of each connection to commonly known or reasonably

[31] Federal Trade Commission, *Start With Security*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed November 7, 2023).
[32] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed November 7, 2023).

foreseeable attacks.

- Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.
- Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.
- Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.
- Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

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

86. Because Plaintiff entrusted Defendant with his PII, Defendant had, and still has, a duty to the Plaintiff to keep his PII secure.

87. Plaintiff reasonably expected that when he provided PII to Defendant and its franchisees and subsidiaries, Defendant would safeguard his PII.

88. Defendant was always fully aware of its obligation to protect the personal and financial data, including Plaintiff's. Defendant was also aware of the significant repercussions if it failed to do so.

89. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data—including Plaintiffs' first name, last name, addresses, and Social Security number, and other highly sensitive and confidential information—constitutes

an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Concrete Injuries are Caused by Defendant's Inadequate Security

90. Plaintiff reasonably expected that Defendant would provide adequate security protections for his PII, and Plaintiff provided Defendant with sensitive, personal information, including his name, address, and Social Security number.

91. Defendant's poor data security deprived Plaintiff of the benefit of his bargain. Plaintiff and other individuals whose PII were entrusted with Defendant understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff received data security services that were of a lesser value than what he reasonably expected. As such, Plaintiff suffered pecuniary injury.

92. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Plaintiff is now, and for the rest of his life will be, at a heightened and substantial risk of identity theft. Plaintiff have also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

93. The cybercriminals who obtained the Plaintiff's PII may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in Plaintiff's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;

- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

94. In addition, if a Plaintiff's Social Security number is used to create false identification for someone who commits a crime, that individual may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

95. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff has been deprived of the value of his PII, for which there is a well-established national and international market.

96. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

97. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[33]

98. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Plaintiff's PII will exploit the data at a later date or re-sell it to other possible exploiters.

99. As a result of the Data Breach, Plaintiff has already suffered injuries, and now faces a substantial and imminent risk of future identity theft.

[33] Susan Ladika, *Study: Data Breaches Pose A Greater Risk* (July 23, 2014), https://www.foxbusiness.com/features/study-data-breaches-pose-a-greater-risk (last accessed November 7, 2023).

Data Breaches Put Consumers at an Increased Risk of Fraud and Identify Theft

100. Data Breaches such as the one experienced Plaintiff is especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

101. The FTC, like the United States Government Accountability Office, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[34]

102. Theft of Private Information is also gravely serious as Private Information is a valuable property right.[35]

> It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which has conducted studies regarding data breaches:" [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[36]

103. PII and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. To be frank, because of Defendant's conduct, Plaintiff must now worry about

[34] *See* https://www.identitytheft.gov/Steps (last accessed November 7, 2023).
[35] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[36] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed November 7, 2023).

identity theft for years on-end.

Plaintiff's Experience

104. Plaintiff is, and at all times relevant to this complaint, a resident and citizen of the State of South Carolina.

105. Plaintiff is an individual who was formerly employed by Defendant. In exchange for employment, Plaintiff was required to provide Defendant with his Private Information, including his Social Security number.

106. Around or after October 27, 2023, Plaintiff received the "Notice to Impacted Individuals" letter dated October 27, 2023, which indicated that Defendant had known about the Data Breach for about 5 months. The letter informed him that his PII was accessed during a cybersecurity incident. The letter stated that the extracted information included information such as his "name", "address", and social security number."[37]

107. Plaintiff is alarmed by the fact that his Social Security number was identified as among the breach data that was accessed.

108. In response to the Data Breach, now that he is finally aware that it occurred over 5 months ago, Plaintiff will be required to spend time dealing with the consequences of the Data Breach, which will continue to include time spent verifying the legitimacy of the Notice to Impacted Individuals, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts.

109. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided Defendant with his PII had Defendant disclosed that it lacked data security practices adequate to safeguard PII.

[37] *See* Notice to Impacted Individuals Letter, attached as Exhibit A.

110. Plaintiff suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant.

111. Plaintiff has already suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

112. Plaintiff reasonably believes that his Private Information may have already been sold by the cybercriminals. Had he been notified of Defendant's breach in a timelier manner, he could have attempted to mitigate his injuries.

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

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

CLASS ACTION ALLEGATIONS

115. Plaintiff brings this case as a class action pursuant to Federal Rule of Civil Procedure 23 on his own behalf and as the Class representatives on behalf of the following:

- **Nationwide Class:** All persons within the United States whose Personal and Private Information was stored on Defendant's computer network systems and who were informed via notice of the company's May 2023 Data Breach.
- **South Carolina Subclass:** All persons within South Carolina whose Personal and Private Information was stored on Defendant's computer network systems and who were informed via notice of the company's May 2023 Data Breach.

116. The Nationwide Class and South Carolina Subclass shall collectively be referred to herein as the "Classes."

117. Plaintiff reserves the right to amend the Class definitions if further investigation and discovery indicate that the Class definitions should be narrowed, expanded, or otherwise modified.

118. Excluded from the Classes are governmental entities, Defendant, its officers, directors, franchise owners, and any entity Defendant retains a controlling interest in; and the affiliates and legal representatives of Defendant.

119. This action has been brought and may be maintained as a class action under Federal Rule of Civil Procedure 23.

120. **Numerosity** – Federal Rule of Civil Procedure 23(a)(1). This Class numbers at least in the thousands of persons. As a result, joinder of all Class Members in a single action is impracticable. Class Members may be informed of the pendency of this class action through a variety of means, including, but not limited to, direct mail, email, published notice, and website posting.

121. **Existence and Predominance of Common Questions of Law and Fact** – Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3). There are questions of fact and law common to the Classes that predominate over any question affecting only individual Members. Those questions, each of which may also be certified under Rule 23(c)(4), include without limitation:

- Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's PII;
- 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;

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant owed a duty to Plaintiff to safeguard his PII;
- Whether Defendant breached its duty to Plaintiff to safeguard his PII;
- Whether computer hackers obtained Plaintiff's PII in the Data Breach;
- Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- Whether Plaintiff suffered legally cognizable damages as a result of Defendant's misconduct;
- Whether Defendant's conduct was negligent;
- Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- Whether Plaintiff is entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

122. **Typicality** – Federal Rule of Civil Procedure 23(a)(3). Plaintiff's claims are typical of those of the Class because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

123. **Superiority** – Federal Rule of Civil Procedure 23(b)(3). A class action is the appropriate method for the fair and efficient adjudication of this controversy. The presentation of separate actions by individual Class Members could create a risk of inconsistent adjudications, establish incompatible standards of conduct for Defendant, and/or substantially impair or impede the ability

of Class Members to protect their interests. In addition, it would be impracticable and undesirable for each member of the Class who suffered an economic loss to bring a separate action. The maintenance of separate actions would place a substantial and unnecessary burden on the courts and could result in inconsistent adjudications, while a single class action can determine, with judicial economy, the rights of all Class Members.

124. **Adequacy** – Federal Rule of Civil Procedure 23(a)(4). Plaintiff is an adequate representative of the Classes because he is a member of the Classes and his interests do not conflict with the interests of the Classes that he seeks to represent. The interests of the Members of the Classes will be fairly and adequately protected by Plaintiff and his undersigned counsel.

125. **Insufficiency of Separate Actions** – Federal Rule of Civil Procedure 23(b)(1). Absent a representative class action, Members of the Classes would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue burden and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated Class members, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Defendant. The proposed Classes thus satisfy the requirements of Fed. R. Civ. P. 23(b)(1).

126. **Declaratory and Injunctive Relief** – Federal Rule of Civil Procedure 23(b)(2). Defendant has acted or refused to act on grounds generally applicable to Plaintiff and the other Members of the Classes, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the Members of the Classes as a whole.

127. Additionally, the Classes may be certified under Rule 23(b)(1) and/or (b)(2) because:

- The prosecution of separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudications with respect to individual members of the Classes that would establish incompatible standards of conduct for the Defendant;
- The prosecution of separate actions by individual members of the Classes would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other members of the Classes not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or
- Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby making appropriate final and injunctive relief with respect to the members of the Classes as a whole.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of the National Class and, alternatively, the Subclass)

128. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

129. As part of the regular course of its business operations Defendant gathered and stored the PII of Plaintiff and Class Members. Plaintiff and the Class were entirely dependent on Defendant to use reasonable measures to safeguard their PII and were vulnerable to the foreseeable harm of a security breach should Defendant fail to safeguard their PII.

130. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and

safeguard their computer property—and Class Members' Private Information held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

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

132. Defendant's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

133. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

134. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result 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 the Class.

135. Defendant gathered and stored the PII of Plaintiff and the Class as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect

commerce.

136. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiff and Class Members and by not complying with applicable industry standards.

137. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard their PII, and by failing to provide prompt notice without reasonable delay.

138. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and those who sought or were employed by it or its franchisees, which is recognized by laws and regulations including but not limited to FTCA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and the Class or minimize the Data Breach.

139. Defendant's multiple failures to comply with applicable laws and regulations, and the violation of Section of 5 of the FTC Act constitutes negligence *per se*.

140. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

141. Defendant had full knowledge of the sensitivity of the PII, the types of harm that Plaintiff could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

142. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class had no ability to protect their PII that was in Defendant's possession.

143. Defendant was in a special relationship with Plaintiff and the Class with respect to the

hacked PII because the aim of Defendant's data security measures was to benefit Plaintiff by ensuring that their PII would remain protected and secure. Only Defendant was able to ensure that its systems were sufficiently secure to protect Plaintiff's and other Class Members' PII. The harm to Plaintiff and the Class from its exposure was highly foreseeable to Defendant.

144. Defendant owed Plaintiff and other Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their PII, including acting to reasonably safeguard such data and providing notification to Plaintiff and the Class of any breach in a timely manner so that appropriate action could be taken to minimize losses.

145. Defendant had duties to protect and safeguard the PII of Plaintiff and other Class Members from being vulnerable to compromise by taking common-sense precautions when dealing with highly sensitive PII. Additional duties that Defendant owed Plaintiff and the Class include:

- Exercising reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that individuals PII was adequately secured from impermissible release, disclosure, and publication;
- To protect Plaintiff's and the Class's PII in its possession by using reasonable and adequate security procedures and systems; and
- To promptly notify Plaintiff and the Class of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PII.

146. Only Defendant was in a position to ensure that its systems and protocols were sufficient

to protect the PII that had been entrusted to them.

147. Defendant breached its duties of care by failing to adequately protect Plaintiff and the Class's PII. Defendant breached its duties by:

- Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the PII in its possession;
- Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;
- Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;
- Failing to adequately train its employees to not store unencrypted PII in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;
- Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's PII;
- Failing to mitigate the harm caused to Plaintiff and the Class;
- Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and
- Failing to promptly notify Plaintiff and other Class Members of the Data Breach that affected their PII.

148. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

149. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in

protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

150. Defendant's failure to provide timely and clear notification of the Data Breach to Plaintiff and the Class prevented Plaintiff and the Class from taking meaningful, proactive steps to securing their PII and mitigating damages.

151. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

152. As a direct and proximate result of Defendant's negligence and negligence *per se*, 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 actual 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 identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain 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 their continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to monitor bank accounts and credit reports, prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

153. As a direct and proximate result of Defendant's negligence, Plaintiff, and members of

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.

154. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and members of 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.

155. Plaintiff and members of the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

COUNT II
Breach of Implied Contract
(On Behalf of the National Class and, alternatively, the Subclass)

156. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

157. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving employment benefits or other services provided by Defendant.

158. Plaintiff and Class Members provided PII to Defendant (or its third-party agents) in exchange for employment benefits and services. In exchange, Defendant promised to protect their PII from unauthorized disclosure.

159. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

160. Implicit in the agreement between Plaintiff, Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable

steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

161. Defendant required Plaintiff and Class Members to provide their PII as part of regular business practices.

162. When Plaintiff and Class Members provided their PII to Defendant as a condition of the employment relationship, implied contracts were created with Defendant. As such, Defendant agreed to reasonably protect such information.

163. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation and belief that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards. Plaintiff and Class Members believed that Defendant would use part of the monies paid to Defendant under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund adequate and reasonable data security practices.

164. Plaintiff and the Class would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures. The safeguarding of Plaintiff's and Class Member's PII was critical to realize the intent of the parties.

165. Plaintiff and Class Members fully performed their obligations under the implied contracts

with Defendant.

166. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII.

167. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and Class Members sustained damages.

168. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

169. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Plaintiff and Class Members for a period longer than the inadequate one-year currently offered.

COUNT III
Unjust Enrichment
(On Behalf of the National Class and, alternatively, the Subclass)

170. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

171. This cause of action is pled in the alternative to Count II.

172. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of employment of Defendant, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such PII held by Defendant.

173. Defendant knew Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

174. Acceptance of the benefit under these facts and circumstances make it inequitable for Defendant to retain that benefit without payment of the value thereof. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members thus suffered as a direct and proximate result of Defendant's decision to prioritize profits over the requisite data security.

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

176. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

177. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

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

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

180. For the benefit of Plaintiff and Class Members, Defendant should be compelled to disgorge proceeds that they unjustly received from them into a common fund or constructive trust.

COUNT IV
Declaratory Judgment
(On Behalf of the National Class and, alternatively, the Subclass)

181. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

182. 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. Furthermore, 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.

183. An actual controversy has arisen in the wake of Defendant's data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff from further data breaches that compromise their PII.

184. Plaintiff alleges that Defendant's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

185. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (i) Defendant continues to owe a legal duty to secure current and former employees' PII and to timely notify employees and former employees of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; (ii) Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' PII.

186. The Court also should issue corresponding prospective injunctive relief requiring that Defendant employ adequate security protocols consistent with law and industry standards to

protect consumers' PII.

187. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach targeted at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach targeted at Defendant occurs, Plaintiffs 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.

188. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs which is targeted at Defendant, Plaintiffs will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost 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.

189. Issuance of the requested injunction will not do a disservice to 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 Plaintiffs and the millions of individuals whose PII would be further compromised.

COUNT V
Breach of Fiduciary Duty
(On Behalf of the National Class and, alternatively, the Subclass)

190. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

191. Defendant had a fiduciary duty to Plaintiff.

192. Plaintiff entrusted Defendant as an employer to keep PII safe and the facts of this case prove the existence of this duty. Such relationship may be created when the facts and

circumstances indicate the party reposing trust in another has some foundation for believing the one so entrusted will act not in his own behalf but in the interest of the party so reposing.

193. Defendant breached this duty by failing to adequately protect Plaintiff's information.

194. This breach of fiduciary duty caused damages to Plaintiff in that his information is now disseminated across the world wide web which subjects his to financial crimes, identity theft, as well as constant worry regarding the use of his information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully request that the Court enter judgment in his favor and against Defendant as follows:

A. For an order certifying the Classes under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as the representatives for the Classes and Plaintiff's attorneys as Class Counsel;

B. For an order declaring the Defendant's conduct violates the causes of action referenced herein;

C. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

D. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an order of restitution and all other forms of equitable monetary relief;

H. For injunctive relief as pleaded or as the Court may deem proper; and

I. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees;

J. Such other and further relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all claims in this Complaint and of any and all issues in this action so triable as of right.

Dated: November 10, 2023

Respectfully Submitted,

/s/ Blake G. Abbott
Paul J. Doolittle (Fed ID #6012)
Blake G. Abbott (Fed ID #13354)
POULIN | WILLEY | ANASTOPOULO, LLC
32 Ann Street
Charleston, SC 29403
Tel: (803) 222-2222
Email:
paul.doolittle@poulinwilley.com
blake.abbott@poulinwilley.com

ClassAction.org
