Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
RALEIGH DIVISION

IN RE: GOLDEN CORRAL DATA BREACH LITIGATION	Case No.: 5:24-cv-00123-M-BM **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Yasmeenah Morrow, Wayland Bennett, Ashley Hunt, Mika Inelus, Amber Walker, and Christie Brooks ("Plaintiffs") bring this Class Action lawsuit on behalf of themselves and on behalf of all others similarly situated (the "Class" or "Class Members"), against Defendant, Golden Corral Corporation ("Golden Corral" or "Defendant"), and allege upon personal information and belief as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action lawsuit against Defendant for its failure to safeguard and protect Plaintiffs' and Class Members' highly sensitive personally identifiable information ("PII")[1] from unauthorized access and exfiltration.[2]

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[2] *See* OFFICE OF THE MAINE ATTORNEY GENERAL, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/d51dd4fd-408e-477f-ae99-7f0ecb058b8e.shtml (last visited June 19, 2024).

2. Defendant failed to implement reasonable and industry standard data security practices to properly secure, safeguard, and destroy Plaintiffs' and Class Members' sensitive PII that it had acquired and stored for Golden Corral's business purposes.

3. As a result of Defendant's failure to implement adequate data security, the highly sensitive PII of approximately 183,272 individuals, including their including their names, Social Security numbers, financial account details, driver's license numbers, medical information, usernames and passwords, and health insurance information (collectively, "Private Information") was accessed and stolen by cybercriminals in a targeted and preventable data breach that took place from August 11, 2024 until August 15, 2024 (the "Data Breach" or "Breach").[3]

4. Despite learning of the Data Breach on August 15, 2023, Golden Corral did not notify victims of the Data Breach that their Private Information was at risk of misuse until on or around February 16, 2024, via Notice of Data Breach Letters it mailed to Plaintiffs and the Class.[4]

5. The Notice of Data Breach Letter sent to Plaintiffs and Class Members confirmed **"an unauthorized actor accessed [Golden Corral's] systems and acquired certain data between August 11, 2023 until August 15, 2023."**[5] Thus, there is no question Plaintiffs' and the Class's Private Information is in the hands of cybercriminals who will undoubtedly use it for nefarious purposes.

6. The Data Breach was a direct result of Defendant's failure to implement adequate

---

[3] *Id.*; *see also* SC MEDIA, *Golden Corral Discloses Data Breach Impacting 180,000 Individuals*, https://www.scmagazine.com/brief/golden-corral-discloses-data-breach-impacting-180000-individuals (last visited June 19, 2024).

[4] *See* OFFICE OF THE MAINE ATTORNEY GENERAL, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/d51dd4fd-408e-477f-ae99-7f0ecb058b8e.shtml (last visited June 19, 2024).

[5] *Id.* (emphasis added).

and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information which it was duty bound to protect.

7. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure Private Information from those risks left that property in a dangerous condition.

8. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (i) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (ii) failing to design, implement, and maintain reasonable data retention policies; (iii) failing to adequately train staff on data security; (iv) failing to comply with industry-standard data security practices; (v) failing to warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (vi) failing to encrypt or adequately encrypt the Private Information; (vii) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (viii) failing to utilize widely available software able to detect and prevent this type of attack, and (ix) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

9. Defendant disregarded the rights of Plaintiffs and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs(s) and Class

Members with prompt and full notice of the Data Breach.

10. In addition, Defendant failed to properly maintain and monitor the computer network and systems that housed the Private Information. Had it properly monitored its data systems it would have discovered the intrusion sooner rather than allowing cybercriminals a four (4) day period of unimpeded access to the Private Information of Plaintiffs and Class Members.

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

12. As a result of the Data Breach, Plaintiffs and Class Members are now at a current, imminent, and ongoing risk of fraud and identity theft. Plaintiffs and Class Members must now and for years into the future closely monitor their credit and financial accounts to guard against identity theft. Such mitigation efforts included and will continue to include in the future, among other things: (i) reviewing financial statements; (ii) changing passwords; and (iii) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

13. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiffs and Class Members have suffered numerous actual and concrete injuries and damages, including: (i) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (iii) financial costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) deprivation of value of their PII; and (vi) the continued risk to their sensitive Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and

adequate measures to protect it collected and maintained.

14. Through this class action lawsuit, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

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

16. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiffs' and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure due to Defendant's negligence.

II. PARTIES

17. **Plaintiff Yasmeenah Morrow** is an individual who is domiciled in Decatur, Alabama. Plaintiff Morrow received a Notice of Data Breach Letter from Defendant advising her that her name, date of birth, and Social Security number were accessed and/or acquired in the Data Breach.

18. **Plaintiff Wayland Bennett** is an individual who is domiciled in Jacksonville, Florida. Plaintiff Bennett received a Notice of Data Breach Letter from Defendant advising him that his name, address, phone number, date of birth, and Social Security number were accessed and/or acquired in the Data Breach.

19. **Plaintiff Ashley Hunt** is an individual who is domiciled in Owingsville, Kentucky. Plaintiff Hunt received a Notice of Data Breach Letter from Defendant advising her that her name and Social Security number were accessed and/or acquired in the Data Breach.

20. **Plaintiff Mika Inelus** is an individual who is domiciled in Jacksonville, Florida. Plaintiff Inelus received a Notice of Data Breach Letter from Defendant notifying her that her name and Social Security number were accessed and/or acquired in the Data Breach.

21. **Plaintiff Amber Walker** is an individual who is domiciled in Theodore, Alabama. Plaintiff received a Notice of Data Breach Letter from Defendant advising her that her name and Social Security number were accessed and/or acquired in the Data Breach.

22. **Plaintiff Christie Brooks** is an individual who is domiciled in Calera, Alabama. Plaintiff received a Notice of Data Breach Letter from Defendant advising her that her name, date of birth, Social Security number, and health insurance information were accessed and/or acquired in the Data Breach.

23. **Defendant Golden Corral Corporation** is a North Carolina corporation with its principal place of business located at 5400 Trinity Rd, Suite 309 Raleigh, NC 27607.

III. JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, some of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

25. This Court has personal jurisdiction over Defendant because it is a North Carolina corporation that operates and has its principal place of business in this District and conducts substantial business in this District.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District, maintains Plaintiffs' and Class Members' Private Information in this District, and has caused harm to Plaintiffs and Class Members in this District.

IV. FACTUAL BACKGROUND

A. Golden Corral's Collection of Plaintiffs' and the Class's Private Information.

27. Based in Raleigh, North Carolina, Golden Corral is a restaurant chain specializing in a buffet dining experience with nearly 400 company-operated and franchise restaurants located in 42 states and serves approximately three million guests per week.[6]

28. According to Golden Corral, it provides job opportunities to approximately 25,000 individuals.[7]

29. Plaintiffs and the Class are comprised of individuals who are current or former employees of Golden Corral and individuals who are or were beneficiaries and/or dependents of individuals who are currently or were formerly employed at Golden Corral.

30. To obtain employment or other benefits from Golden Corral, Plaintiffs and Class Members were required to provide their Private Information to Golden Corral.

31. As part of the services and employment Defendant provides, it was entrusted with, and obligated to safeguard and protect the Private Information of its employees and their beneficiaries and/or dependents, such as Plaintiffs and the Class, in accordance with all applicable laws and industry standards.

---

[6] GOLDEN CORRAL, Golden Corral Culture, https://www.goldencorral.com/careers/culture/ (last visited June 19, 2024).

[7] *Id.*

32. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

33. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Plaintiffs' and Class Members' Private Information, Defendant could not operate its business and obtain revenue.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

35. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties.

36. Defendant has a legal duty to keep Plaintiffs' and the Class Members' Private Information safe and confidential.

37. Defendant had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

38. Indeed, Defendant made promises and representations that the Private Information it collected from them would be kept safe, confidential, that the privacy of that information would be maintained.[8]

39. Defendant's Privacy Policy on its website states in part as follows:

> Security of your information is very important to us, and we have put in place reasonable safeguards to preserve the integrity and security of the information we collect and share

[8] GOLDEN CORRAL, Privacy Policy, https://www.goldencorral.com/privacy/ (last visited June 19, 2024).

> with our service providers. However, no security system is perfect, and we cannot guarantee the security of our systems at all times. If any personal information under our control is compromised because of a data security breach, we will take steps to investigate the situation and, if appropriate, notify those individuals whose information may have been compromised, and take additional steps in accordance with any applicable laws and regulations.[9]

B. Golden Corral's Massive and Preventable Data Breach.

40. It is clear Golden Corral did not "put in place reasonable safeguards to preserve the integrity and security of the information [it] collect[s]," as asserted by its Privacy Policy, because on or about August 15, 2023, Golden Corral experienced a data breach that impacted its computer systems and caused a temporary disruption to its corporate operations.[10]

41. After an investigation, Golden Corral learned that an unauthorized actor accessed its systems and may have viewed or acquired certain business data between August 11, 2023 until August 15, 2023.[11]

42. On or around February 16, 2024, Golden Corral began sending Notice of Data Breach Letters to individuals impacted by the Data Breach, which state in pertinent part as follows:

> Golden Corral Corporation ("Golden Corral") writes to make you aware of a recent incident that may impact the privacy of some of your information. We are providing you with notice of the incident, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.
>
> **What Happened.** On or about August 15, 2023, Golden Corral experienced a data security incident that caused a temporary disruption to our corporate operations. We promptly responded and launched an investigation to confirm the nature and scope of the incident and restore impacted computer systems to operability. **Through the investigation, we learned that an unauthorized actor accessed our**

[9] *Id.*

[10] *See* OFFICE OF THE MAINE ATTORNEY GENERAL, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/d51dd4fd-408e-477f-ae99-7f0ecb058b8e.shtml (last visited June 19, 2024).

[11] *Id.*

systems and acquired certain data between August 11, 2023 until August 15, 2023. We conducted a thorough review of the data that was potentially viewed or acquired to determine whether it contained any sensitive information. We concluded our review and determined that information related to you was included in the potentially impacted data set. After determining the scope of information in the potentially impacted files, we undertook efforts to locate address information for the affected individuals. That review process completed on January 26, 2024. We then put resources in place to assist and provide this direct notice.

What Information Was Involved. The information that may be present in the files viewed or acquired as a result of this incident could include your name and [Extra1].[12] What We Are Doing. We treat our responsibility to safeguard the information entrusted to us as an utmost priority. As such, we responded promptly to this incident and have been working diligently to provide you with an accurate and complete notice of the incident. Our immediate response to this event also included prompt and continued correspondence with federal law enforcement authorities. As part of our ongoing commitment to the privacy and security of information in our care, we reviewed our existing policies and procedures relating to data protection and security. As an added precaution, we are providing you with 24 months of complimentary access to credit monitoring and identity restoration services through Experian, as well as guidance on how to better protect your information. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included within the enclosure to this letter.

What You Can Do. You can find out more about how to safeguard your information in the enclosed Steps You Can Take to Help Protect Personal Information. There, you will find additional information about the complimentary credit monitoring and identity restoration services we are offering and how to enroll. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months.[13]

43. The Private Information accessed or acquired in the Data Breach included sensitive information such as: names, Social Security numbers, financial account details, driver's license numbers, medical information, usernames and passwords, and health insurance information.[14]

[12] The information exposed in the Data Breach varied by individual.

[13] *Id.* (emphasis added).

[14] GBHACKERS ON SECURITY, *Golden Corral Restaurant Chain Hacked: 180,000+ Users' Data Stolen*, https://gbhackers.com/golden-corral-restaurant-chain-hacked/ (last visited June 19, 2024).

44. The Notice of Data Breach Letter confirmed "an unauthorized actor accessed [Golden Corral's] systems and acquired certain data between August 11, 2023 until August 15, 2023."[15]

45. Because Golden Corral made the admission above, there is no question Plaintiffs' and the Class's Private Information is in the hands of cybercriminals who will undoubtedly use their Private Information for nefarious purposes or sell it on the Dark Web.

C. Defendant Knew the Risks of Storing Valuable PII and the Foreseeable Harm to Victims.

46. At all relevant times, Defendant knew it was storing sensitive PII and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

47. Defendant also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

48. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

49. Private Information has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[16]

---

[15] *See* OFFICE OF THE MAINE ATTORNEY GENERAL, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/d51dd4fd-408e-477f-ae99-7f0ecb058b8e.shtml (last visited June 19, 2024).

[16] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/(last visited June 19, 2024).

50. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the ITRC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[17]

51. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[18]

52. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and the Class especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

53. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n 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 [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that

[17] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.

[18] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).

attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[19]

54. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

D. Defendant Breached its Duty to Protect Plaintiffs and Class Member's PII.

55. Defendant agreed to and undertook legal duties to maintain the personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"). Under state and federal law, businesses like Defendant have duties to protect its current and former employee's PII and to notify them about data breaches.

56. The Private Information held by Defendant in its computer system and network included the highly sensitive Private Information of Plaintiffs and Class Members.

57. On August 15, 2023, Defendant discovered a ransomware attack on its inadequately protected computer systems.

58. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands

[19] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [20] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[21]

59. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[22] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

60. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[23] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[24] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[25] And even where companies pay for the return of data attackers

[20] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed January 2, 2024).
[21] *Id.*
[22] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends
[23] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/
[24] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report
[25] *Id.*

often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[26]

61. After an investigation, Defendant disclosed that **an unauthorized actor not only accessed its systems, but acquired certain data**, including the PII of Plaintiffs and the Class, between August 11, 2023, and August 15, 2023.[27]

62. Despite learning of the Data Breach in August 2023, Defendant did not notify the victims of the Data Breach until months later in February 2024.[28] In other words, criminals had a months-long head-start in using Plaintiffs' and the Class's data for nefarious purposes.

63. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, and its failure to follow its own policies, in order to protect Plaintiffs and Class Member's PII.

E. Plaintiffs' Individual Experiences.

Plaintiff Wayland Bennett

64. Plaintiff Bennett received a Notice of Data Breach Letter from Defendant informing him that his highly confidential Private Information was compromised in the Data Breach.

65. Defendant was in possession of Plaintiff Bennet's Private Information before, during, and after the Data Breach.

66. Because of the Data Breach, there is no doubt Plaintiff Bennett's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach

---

[26] *Id.*

[27] *See* OFFICE OF THE MAINE ATTORNEY GENERAL, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/d51dd4fd-408e-477f-ae99-7f0ecb058b8e.shtml (last visited June 19, 2024).

[28] *Id.*

Letter from Defendant not only disclosed that an unauthorized third-party had ***accessed*** Defendant's systems, but it ***confirmed*** that the unauthorized criminal actor ***acquired*** highly sensitive PII.[29] As such, Plaintiff Bennett and the Class are at an imminent risk of identity theft and fraud.

67. Plaintiff Bennett has already experienced misuse of his Private Information due to the Data Breach. After the Data Breach, Plaintiff Bennett suffered unauthorized charges to his financial account. This is hardly a coincidence. When Social Security numbers are exposed in a data breach, such is the case here, cybercriminals can use this information to access existing bank accounts.[30] The fraud and identity theft Plaintiff Bennett suffered has detrimentally impacted Plaintiff Bennett's life as a whole and has caused immense financial strain on him as a direct result of the Data Breach.

68. To make matters worse, Plaintiff Bennett has also experienced misuse of his Private Information in the form of increased spam calls and text messages post Data Breach. Prior to the Data Breach, Plaintiff Bennett was not experiencing spam calls and text messages of this frequency.

---

[29] https://apps.web.maine.gov/online/aeviewer/ME/40/d51dd4fd-408e-477f-ae99-7f0ecb058b8e.shtml ("Through the investigation, we learned that an unauthorized actor accessed our systems and acquired certain data between August 11, 2023 until August 15, 2023.").

[30] *See, e.g.,* https://surfshark.com/blog/what-can-someone-do-with-your-ssn ("An identity thief can use your SSN together with your PII to open new bank accounts or access existing ones, take out credit cards, and apply for loans all in your name."); https://www.aura.com/learn/what-can-someone-do-with-your-social-security-number#3.-Empty-your-bank-account ("Many banks will use your SSN as a primary identifier when you call for help or try to make changes to your account. With your account number and SSN (which can often be found together after data breaches), fraudsters can access your account, add themselves as a user, or transfer out your savings using digital wallets like Zelle and Cash App."); https://www.marca.com/en/lifestyle/us-news/personal-finance/2023/08/06/64cf8b84268e3ed0448b45d0.html (The list of actions someone can carry out if they get hold of your social security number include:… [e]mpty your bank account.").

69. As a result of the Data Breach, Plaintiff Bennett has already expended hours of his time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

70. Plaintiff Bennett places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Bennett has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

71. Plaintiff Bennett has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and increased risk of future harm Plaintiff Bennett and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Bennett and the Class.

72. Knowing that thieves intentionally targeted and stole his Private Information, including his Social Security number, and knowing that his Private Information is in the hands of cybercriminals has caused Plaintiff Bennett great anxiety beyond mere worry. Specifically, Plaintiff Bennett has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that his Private Information has been stolen.

73. Plaintiff Bennett has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs' and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

74. Plaintiff Bennett has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of his valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by his Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of his Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Bennett should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect his Private Information; and (v) continued risk to his Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Amber Renee Walker

75. Plaintiff Walker received a Notice of Data Breach Letter from Defendant informing her that her highly confidential Private Information was compromised in the Data Breach.

76. Defendant was in possession of Plaintiff Walker's Private Information before, during, and after the Data Breach.

77. Because of the Data Breach, there is no doubt Plaintiff Walker's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach Letter from Defendant not only disclosed that an unauthorized third-party had ***accessed*** Defendant's systems, but it ***confirmed*** that the unauthorized criminal actor ***acquired*** highly

sensitive PII. As such, Plaintiff Walker and the Class are at an imminent risk of identity theft and fraud.

78. Plaintiff Walker has already experienced misuse of her Private Information due to the Data Breach. Plaintiff Walker has suffered numerous incidents of unauthorized hard inquiries to her credit that are not in relation to any credit she applied for. These unauthorized hard inquiries have caused her credit scores to decline. The fraud and identity theft Plaintiff Walker suffered has detrimentally impacted Plaintiff Walker's life as a whole and has caused immense financial strain on her as a direct result of the Data Breach. There is no doubt Plaintiff Walker's PII is now on the Dark Web as a result of the Data Breach.

79. To make matters worse, Plaintiff Walker has also experienced misuse of her Private Information in the form of spam calls, text messages, and phishing emails post Data Breach.

80. As a result of the Data Breach, Plaintiff Walker has already expended hours of her time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

81. Plaintiff Walker places significant value in the security of her Private Information and does not readily disclose it. Plaintiff Walker has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

82. Plaintiff Walker has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and

increased risk of future harm Plaintiff Walker and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Walker and the Class.

83. Knowing that thieves intentionally targeted and stole her Private Information, including her Social Security number, and knowing that her Private Information is in the hands of cybercriminals has caused Plaintiff Walker great anxiety beyond mere worry. Specifically, Plaintiff Walker has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her Private Information has been stolen.

84. Plaintiff Walker has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs' and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

85. Plaintiff Walker has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of her valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by her Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of her Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff Walker should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect her Private Information; and (v) continued risk to her Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as

Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Christie Brooks

86. Plaintiff Brooks received a Notice of Data Breach Letter from Defendant informing her that her highly confidential Private Information was compromised in the Data Breach.

87. Defendant was in possession of Plaintiff Brooks's Private Information before, during, and after the Data Breach.

88. Because of the Data Breach, there is no doubt Plaintiff Brooks's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach Letter from Defendant not only disclosed that an unauthorized third-party had accessed Defendant's systems, but it confirmed that the unauthorized criminal actor acquired highly sensitive PII. As such, Plaintiff Brooks and the Class are at an imminent risk of identity theft and fraud.

89. Plaintiff Brooks has already experienced misuse of her Private Information due to the Data Breach. On June 4, 2024, Plaintiff Brooks was notified by Experian that several pieces of her Private Information, including her Social Security number, were found on the Dark Web.

90. To make matters worse, Plaintiff Brooks has also experienced misuse of her Private Information in the form of spam calls, text messages, and phishing emails post Data Breach. Plaintiff Brooks has experienced a dramatic increase in spam and scam phone calls and emails as a result of the Data Breach.

91. As a result of the Data Breach, Plaintiff Brooks has already expended **over 20 hours** of her time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including

investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

92. Plaintiff Brooks places significant value in the security of her Private Information and does not readily disclose it. Plaintiff Brooks has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

93. Plaintiff Brooks has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and increased risk of future harm Plaintiff Brooks and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Brooks and the Class.

94. Knowing that thieves intentionally targeted and stole her Private Information, including her Social Security number, and knowing that her Private Information is in the hands of cybercriminals has caused Plaintiff Brooks great anxiety beyond mere worry. Specifically, Plaintiff Brooks has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her Private Information has been stolen.

95. Plaintiff Brooks has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs' and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

96. Plaintiff Brooks has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of her valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by her Private

Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of her Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff Brooks should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect her Private Information; and (v) continued risk to her Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

97. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Brooks to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

Plaintiff Yasmeenah Morrow

98. Plaintiff Morrow received a Notice of Data Breach Letter from Defendant informing her that her highly confidential Private Information was compromised in the Data Breach.

99. Defendant was in possession of Plaintiff Morrow's Private Information before, during, and after the Data Breach.

100. Because of the Data Breach, there is no doubt Plaintiff Morrow's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of

Data Breach Letter from Defendant not only disclosed that an unauthorized third-party had ***accessed*** Defendant's systems, but it ***confirmed*** that the unauthorized criminal actor ***acquired*** highly sensitive PII. As such, Plaintiff Morrow and the Class are at an imminent risk of identity theft and fraud.

101. Plaintiff Morrow has also experienced misuse of her Private Information in the form of spam calls, text messages, and phishing emails post Data Breach. Plaintiff Morrow has experienced a dramatic increase in spam and scam phone calls and emails as a result of the Data Breach.

102. As a result of the Data Breach, Plaintiff Morrow has already expended hours of her time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

103. Plaintiff Morrow places significant value in the security of her Private Information and does not readily disclose it. Plaintiff Morrow has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

104. Plaintiff Morrow has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and increased risk of future harm Plaintiff Morrow and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Morrow and the Class.

105. Knowing that thieves intentionally targeted and stole her Private Information, including her Social Security number, and knowing that her Private Information is in the hands of cybercriminals has caused Plaintiff Morrow great anxiety beyond mere worry. Specifically, Plaintiff Morrow has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her Private Information has been stolen.

106. Plaintiff Morrow has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs' and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

107. Plaintiff Morrow has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of her valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by her Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of her Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff Morrow should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect her Private Information; and (v) continued risk to her Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Ashley Hunt

108. Plaintiff Hunt received a Notice of Data Breach Letter from Defendant informing her that her highly confidential Private Information was compromised in the Data Breach.

109. Defendant was in possession of Plaintiff Hunt's Private Information before, during, and after the Data Breach.

110. Because of the Data Breach, there is no doubt Plaintiff Hunt's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach Letter from Defendant not only disclosed that an unauthorized third-party had ***accessed*** Defendant's systems, but it ***confirmed*** that the unauthorized criminal actor ***acquired*** highly sensitive PII. As such, Plaintiff Hunt and the Class are at an imminent risk of identity theft and fraud.

111. Plaintiff Hunt has also experienced misuse of her Private Information in the form of spam calls, text messages, and phishing emails post Data Breach.

112. As a result of the Data Breach, Plaintiff Hunt has already expended hours of her time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

113. Plaintiff Hunt places significant value in the security of her Private Information and does not readily disclose it. Plaintiff Hunt has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

114. Plaintiff Hunt has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real

and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and increased risk of future harm Plaintiff Hunt and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Hunt and the Class.

115. Knowing that thieves intentionally targeted and stole her Private Information, including her Social Security number, and knowing that her Private Information is in the hands of cybercriminals has caused Plaintiff Hunt great anxiety beyond mere worry. Specifically, Plaintiff Hunt has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her Private Information has been stolen.

116. Plaintiff Hunt has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs' and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

117. Plaintiff Hunt has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of her valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by her Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of her Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security-i.e., the difference in value between what Plaintiff Hunt should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect her Private Information; and (v) continued risk to her Private Information, which

remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Mika Inelus

118. Plaintiff Inelus received a Notice of Data Breach Letter from Defendant informing her that her highly confidential Private Information was compromised in the Data Breach.

119. Defendant was in possession of Plaintiff Inelus's Private Information before, during, and after the Data Breach.

120. Because of the Data Breach, there is no doubt Plaintiff Inelus's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach Letter from Defendant not only disclosed that an unauthorized third-party had ***accessed*** Defendant's systems, but it ***confirmed*** that the unauthorized criminal actor ***acquired*** highly sensitive PII. As such, Plaintiff Inelus and the Class are at an imminent risk of identity theft and fraud.

121. As a result of the Data Breach, Plaintiff Inelus has already expended hours of her time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that she is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

122. Plaintiff Inelus places significant value in the security of her Private Information and does not readily disclose it. Plaintiff Inelus has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

123. Plaintiff Inelus has also experienced misuse of her Private Information in the form of spam calls and text messages that reference fraud concerning her Zelle account and bank account.

124. Plaintiff Inelus has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and increased risk of future harm Plaintiff Inelus and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Inelus and the Class.

125. Knowing that thieves intentionally targeted and stole her Private Information, including her Social Security number, and knowing that her Private Information is in the hands of cybercriminals has caused Plaintiff Inelus great anxiety beyond mere worry. Specifically, Plaintiff Inelus has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her Private Information has been stolen.

126. Plaintiff Inelus has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs' and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

127. Plaintiff Inelus has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of her valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by her Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of her Private Information; (iv) loss of the benefit of the bargain with Defendant to provide

adequate and reasonable data security—i.e., the difference in value between what Plaintiff Inelus should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect her Private Information; and (v) continued risk to her Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

F. Plaintiffs and Class Members Suffered Damages.

128. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. Plaintiffs and Class Members must immediately devote time, energy, and money to: (i) closely monitor their statements, bills, records, and credit and financial accounts; (ii) change login and password information on any sensitive account even more frequently than they already do; (iii) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (iv) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

129. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct.

130. Further, the value of Plaintiffs' and Class Members' PII has been diminished by its exposure in the Data Breach.

131. As a result of Defendant's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of Private Information.

132. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[31]

133. Plaintiffs and the Class Members have also been injured by Defendant's unauthorized disclosure of their confidential PII.

134. Plaintiffs and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect Plaintiffs and Class Member's Private Information.

G. Common Injuries and Damages.

135. As result of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

136. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including but not limited to: (i) invasion of privacy; (ii) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft

[31] *See* https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.

risk; (iv) "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) the loss of benefit of the employment bargain; (viii) diminution of value of their Private Information; and (ix) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

H. The Risk of Identity Theft to Plaintiffs and Class Members is Present and Ongoing.

137. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market (or Dark Web) to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

138. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

139. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

140. The Dark Web is an unindexed layer of the internet that requires special software or authentication to access.[32] Criminals in particular favor the Dark Web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the Dark Web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[33] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

141. A sophisticated black market exists on the Dark Web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[34] The digital character of PII stolen in data breaches lends itself to Dark Web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[35] As Microsoft warns "[t]he anonymity of the Dark Web lends itself well to those who would seek to do financial harm to others."[36]

---

[32] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[33] *Id.*

[34] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

[35] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[36] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

142. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious 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.[37]

143. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive 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.

144. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[38]

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

---

[37] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

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

official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[39]

146. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[40]

147. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[41] Defendant did not rapidly report to Plaintiffs and the Class that their Private Information had been stolen.

148. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

149. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to

[39] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[40] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

[41] *Id.*

spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

150. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

151. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[42]

152. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (i) encrypting information stored on computer networks; (ii) retaining payment card information only as long as necessary; (iii) properly disposing of personal information that is no longer needed; (iv) limiting administrative access to business systems; (v) using industry-tested and accepted methods for securing data; (vi) monitoring activity on networks to uncover unapproved activity; (vii) verifying that privacy and security features function properly; (viii) testing for common

[42] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

vulnerabilities; and (ix) updating and patching third-party software.[43]

153. The FTC treats 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(a) of the FTC Act.[44]

154. Defendant's failure to timely notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' 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.

I. Loss of Time to Mitigate the Risk of Identify Theft and Fraud.

155. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

156. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and

[43] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[44] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices.

filing police reports, which may take years to discover and detect.

157. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[45] Indeed, the FTC recommends that identity theft victims take several steps and spend time 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.[46]

J. Diminution of Value of the Private Information

158. PII is a valuable property right.[47] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

---

[45] *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 ("GAO Report").

[46] *See* https://www.identitytheft.gov/Steps.

[47] *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).

159. Private Information can sell for as much as $363 per record according to the Infosec Institute.[48]

160. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[49] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[50, 51] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[52]

161. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

K. Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary.

162. To date, Defendant has done nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant has not offered any relief or protection. Instead, Defendant offered guidance on how to better protect against identity theft or fraud. This is a tacit admission that its failure to protect their Private Information has caused Plaintiffs and Class great injuries.

---

[48] *See* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[49] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[50] https://datacoup.com/.

[51] https://digi.me/what-is-digime/.

[52] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

163. Defendant also places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for services, as opposed to automatically enrolling all victims of this Data Breach.

164. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – *e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

165. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

166. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[53] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

167. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of

[53] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

fraud and identity theft for many years into the future.

168. The retail cost of credit monitoring and identity theft monitoring can cost $200.00 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five (5) years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

L. Injunctive Relief is Necessary to Protect Against Future Data Breaches

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

170. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, she suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Private Information; and

h. continued risk to their Private Information —which remains in Defendant's possession—and is thus at risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

M. Lack of Compensation

171. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

172. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

173. Further, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

174. Specifically, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

175. In addition, Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the property of loss of value damages in related cases.

176. Plaintiffs and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed

to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

177. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of Private Information. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach and did not timely notify all victims. They have yet to offer an explanation of purpose for the delay. This delay violates notification requirements and increases the injuries to Plaintiffs(s) and Class.

V. CLASS ALLEGATIONS

178. Plaintiffs brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following Nationwide class (the "Class"):

> **All individuals in the United States whose Private Information was compromised in the Defendant's Data Breach.**

179. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

180. Plaintiffs reserves the right to modify or amend the definition of the proposed Class(es) prior to moving for class certification.

181. **Numerosity.** The classes described above are so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this

Court. The exact size of the Classes and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

182. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had a duty to maintain the confidentiality of Plaintiffs and Class Members' Private Information;

c. Whether Defendant breached its obligation to maintain Plaintiffs and the Class Members' private information in confidence;

d. Whether Defendant was negligent in collecting, storing and safeguarding Plaintiffs' and Class Members' Private Information, and breached its duties thereby;

e. Whether Defendant breached its fiduciary duty to Plaintiffs and the Class.

f. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

g. Whether Plaintiffs and Class Members are entitled to restitution or disgorgement as a result of Defendant's wrongful conduct; and

h. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

183. **Typicality**. Plaintiffs' claims are typical of the claims of the Class Members. The claims of the Plaintiffs and members of the Classes are based on the same legal theories and arise from the same failure by Defendant to safeguard Private Information. Plaintiffs and Class

Members' information was stored by Defendant's software, each having their Private Information obtained by an unauthorized third party.

184. **Adequacy of Representation.** Plaintiffs is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members she seeks to represent; Plaintiffs has retained counsel competent and experienced in complex class action litigation; Plaintiffs intends to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

185. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class Members. For example, Defendant's liability and the fact of damages is common to Plaintiffs and each member of the Classes. If Defendant breached its common law and statutory duties to secure Private Information on its network server, then Plaintiffs and each Class Member suffered damages from the exposure of sensitive Private Information in the Data Breach.

186. **Superiority.** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits, making this action superior to individual actions.

187. **Manageability.** The precise size of the Classes is unknown without the disclosure of Defendant's records. The claims of Plaintiffs and the Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiffs and the Classes.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

188. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

189. Golden Corral solicited, gathered, and stored the Private Information of Plaintiffs and Class Members.

190. Upon accepting and storing the Private Information of Plaintiffs and Class Members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiffs and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

191. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

192. Because of this special relationship, Defendant required Plaintiffs and Class Members to provide their Private Information, including names, Social Security numbers, and other Private Information.

193. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiffs and Class Members in its possession was only used for the provided

purpose and that Defendant would destroy any Private Information that it was not required to maintain.

194. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness.

195. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiffs' and Class Members' Private Information from being foreseeably accessed, and its improper retention of Private Information it was not required to maintain, Defendant negligently failed to observe and perform its duty.

196. Plaintiffs and Class Members did not receive the benefit of the bargain with Defendant, because providing their Private Information was in exchange for Defendant's implied agreement to secure and keep it safe and to delete it once no longer required.

197. Defendant was aware of the fact that cybercriminals routinely target large corporations through cyberattacks in an attempt to steal customer and employee Private Information. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

198. Defendant owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

199. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the

actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

200. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and

d. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

201. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the Private Information that Plaintiffs and the Class had entrusted to it.

202. Plaintiffs' injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

203. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's Private Information;

d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

e. Failing to promptly notify Plaintiffs and Class Members of the Data Breach that affected their Private Information.

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

205. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

206. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Class Members while it was within Defendant's possession and control.

207. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

208. Plaintiffs and Class Members could have taken actions earlier had they been timely notified of the Data Breach.

209. Plaintiffs and Class Members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

210. Plaintiffs and Class Members have suffered harm from the delay in notifying them of the Data Breach.

211. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiffs and Class Members have suffered, as Plaintiffs have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses;

(vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

212. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

213. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Classes)

214. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

215. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and the Class.

216. 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 Private Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

217. Defendant gathered and stored the Private Information of Plaintiffs and the Class as part of its business, which solicitations and services affect commerce.

218. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

219. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

220. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

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

222. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

223. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's Private Information.

224. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

225. Defendant's violations of the FTC Act constitute negligence *per se*.

226. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

227. The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

228. Plaintiffs and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Classes)

229. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

230. Defendant offered employment, compensation, and other elective benefits to Plaintiffs and Class Members in exchange for their Private Information and labor.

231. Defendant required Plaintiffs and Class Members to provide their Private Information, including names and Social Security numbers, and other personal information. In exchange Defendant promised to keep the Private Information of Plaintiffs and Class Members safe from unauthorized access and to delete or destroy the Private Information once the employment relationship ended or it was no longer necessary to maintain the Private Information.

232. Plaintiffs and Class Members, had they known that Defendant would not keep their Private Information secure or that Defendant would continue to possess it for years after their employment ended, would have demanded higher pay or chosen to take other employment and not be employed by Defendant.

233. Implied in these exchanges was a promise by Defendant to ensure that the Private

Information of Plaintiffs and Class Members in its possession was only used to provide the agreed-upon compensation and other elective employment benefits from Defendant.

234. These exchanges constituted an agreement between the Parties: Plaintiffs and Class Members would provide their Private Information for a limited period of time in exchange for employment and benefits provided by Defendant. No reasonable person would have provided their Private Information to Defendant without a promise to safeguard it and no reasonable person would have provided their Private Information to Defendant to retain for its own uses for years after the employment ended.

235. These agreements were made with Plaintiffs as an inducement to being employed by Defendant.

236. It is clear from these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class Members would not have disclosed their Private Information to Defendant but for Defendant's promise of compensation and other employment benefits and Defendant promise to safeguard and delete their Private Information. Defendant presumably would not have taken Plaintiffs' and Class Members' Private Information if it did not intend to provide Plaintiffs and Class Members compensation and other employment benefits. Nor could Defendant reasonably infer from the circumstances of the transaction that safeguarding the Private Information was a not necessary obligation or that it could maintain the Private Information for purposes unrelated to employment, i.e., after the relationship ended.

237. Defendant was therefore required to reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure and/or use and to delete it following the end of the employment relationship.

238. Plaintiffs and Class Members accepted Defendant's employment offer and fully

performed their obligations under the implied contract with Defendant by providing their Private Information, directly or indirectly, to Defendant, among other obligations.

239. Plaintiffs and Class Members would not have provided and entrusted their Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information for uses other than compensation and other employment benefits from Defendant.

240. Plaintiffs and Class Members did not provide their Private Information for non-employment purposes and Defendant had no reason to retain it following the end of the employment term

241. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' Private Information.

242. Defendant's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties: Plaintiffs' and Class Members' employment in exchange for compensation and benefits.

243. Defendant was on notice that its systems could be vulnerable to unauthorized access yet failed to invest in proper safeguarding of Plaintiffs' and Class Members' Private Information.

244. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class Members' Private Information, which Plaintiffs and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and Class Members.

245. While Defendant had discretion in the specifics of how it met the applicable laws and industry and contractual standards, this discretion was governed by an implied covenant of good faith and fair dealing.

246. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations when it engaged in unlawful practices under other laws. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' Private Information; storing the Private Information of former employees despite any valid purpose for the storage thereof ceasing upon terminating the relationship with those individuals; and failing to disclose to Plaintiffs and Class Members at the time they provided their Private Information to it that Defendant's data security systems, including training, auditing, and testing of employees, improperly retained the Private Information of Plaintiffs and Class Members after it was no longer necessary, and failed to meet applicable legal and industry standards.

247. Plaintiffs and Class Members did all or substantially all the significant things that the contract required them to do.

248. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiffs and the Class Members suffered injury as described in detail in this complaint and are entitled to damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Classes)

249. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

250. Plaintiffs bring this claim in the alternative to the breach of contract claim above.

251. Plaintiffs and the Class Members conferred a monetary benefit on Defendant by providing their Private Information which Defendant required as a condition of their employment.

Plaintiffs and Class Members provided their Private Information and accepted employment on the condition that Defendant safeguard their Private Information and delete it once it was no longer required to retain it.

252. Plaintiffs and Class Members conferred a monetary benefit on Defendant in that Defendant derived revenue from their labor, a precondition of which required Plaintiffs and Class Members to entrust their Private Information to Defendant. Without the labor and Private Information provided by Plaintiffs and Class Members, Defendant could not derive revenue from its regular business activities. A portion of the revenue derived from the labor and Private Information of Plaintiffs and Class Members was to be used to provide a reasonable level of data security and practices, and the amount of revenue to be allocated to data security is known to Defendant.

253. Defendant knew that Plaintiffs and Class Members conferred a benefit on it and Defendant accepted that benefit. Defendant derived revenue from the labor and Private Information of Plaintiffs and the Class and rather than use a portion of that revenue to protect the Private Information of Plaintiffs and the Class it instead diverted that money to its own profit.

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

255. Under the principles of equity and good conscience, Defendant should not be permitted to retain the profits it wrongfully derived from Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

256. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided. Defendant has money in its hands that in equity and good conscience, it should not be permitted to retain.

257. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged and that it diverted money intended to protect Plaintiffs and the Class to its own profits.

258. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information or labor to Defendant.

259. Plaintiffs and Class Members have no adequate remedy at law.

260. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and

recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

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

FIFTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiffs and the Classes)

263. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

264. As previously alleged and pleaded, Defendant owes duties of care to Plaintiffs and Class Members that require it to adequately secure their Private Information.

265. Defendant still possesses the Private Information of Plaintiffs and the Class Members even after their employment relationship ended and Defendant was no longer required to maintain it.

266. Defendant has not satisfied its obligations and legal duties to Plaintiffs and the Class Members.

267. According to the Notice Letter, Defendant is taking some steps to increase its data security but it is unclear whether those steps are adequate or whether Defendant intends to retain ex-employee Private Information. Moreover, there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Data Breach, and to once again place profits above protection.

268. Plaintiffs, therefore, seek a declaration that (i) Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security; and (ii) to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

b. Ordering Defendant to significantly increase its spending on cybersecurity, including systems and personnel;

c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner any Private Information not necessary for its provisions of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

h. Ordering Defendant to implement and enforce adequate retention policies for Private Information, including destroying Private Information as soon as it is no longer necessary for it to be retained;

i. Ordering Defendant to meaningfully educate its employees about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves; and

j. Ordering that Defendant remove former employees' Private Information from any hard drive or server that has external (Internet) access.

SIXTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Classes)

269. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

270. In light of the special relationship between Defendant, as an employer, and Plaintiffs and Class Members, Defendant became a fiduciary by undertaking a guardianship of

Plaintiffs' and Class Members' Private Information.

271. An employer has a fiduciary duty to not disclose an employee's Private Information.

272. Defendant became a fiduciary, created by its undertaking and guardianship of Plaintiffs' and the Class Members' Private Information, to act primarily for the benefit of Plaintiffs and Class Members.

273. This duty included the obligation and responsibility to:

a. safeguard Plaintiffs' and Class Members' Private Information;

b. timely detect and notify Plaintiffs and the Class in the event of a data breach;

c. only utilize vendors with adequate data security infrastructure, procedures, and protocols;

d. establish and implement appropriate oversight and monitoring procedures for the activities of its vendors.

274. In order to provide employment or other elective benefits to Plaintiffs and Class Members, Defendant required that Plaintiffs and Class Members provide their Private Information to Golden Corral.

275. Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiffs' and Class Members' Private Information, for the benefit of Plaintiffs and Class Members and in order to provide Plaintiffs and Class Members with employment and/or other elective benefits.

276. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with them.

277. Defendant breached the fiduciary duties it owed to Plaintiffs and Class Members

by failing to protect Plaintiffs' and Class Members' Private Information.

278. Defendant further breached the fiduciary duties it owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach and by utilizing inadequate data security infrastructure, procedures, and protocols.

279. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer concrete injury, including, but not limited to: (i) actual misuse of their Private Information in the form of identity theft and fraud; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, time and effort spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

280. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grants the following:

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

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

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

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

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

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

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

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

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

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

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

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

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

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

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

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

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

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

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

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

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

VII. JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Date: June 20, 2024

Respectfully Submitted,

/s/: Gary M. Klinger

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: 866-252-0878
Fax: 865-522-0049
gklinger@milberg.com
Interim Lead Class Counsel

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

William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

Philip J. Krzeski
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
pkrzeski@chestnutcambronne.com

Todd S. Garber
FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com

Daniel Srourian
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: (213) 474-3800
Facsimile: (213) 471-4160
Email: daniel@slfla.com

Plaintiffs' Executive Committee

CERTIFICATE OF SERVICE

I hereby certify that all counsel of record who are deemed to have consented to electronic service are being served on June 20, 2024 with a copy of this document via the Court's CM/ECF system.

/s/: Gary M. Klinger
Gary M. Klinger