EXHIBIT B

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JUSTIN SHERWOOD; LINDSEY QUAN; TABATHA BEDONT F/K/A TABATHA JOHNSON; GREG TORRANO; JENNIFER HILL; SIA MOODY; ANTHONY RUIZ; ALICE DODD, FREDERICK LEWIS; DOUGLAS ACKMAN; RYAN EVANS; AMBER THOMAS; AND MARIA CHAVEZ, individually and on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

HORIZON ACTUARIAL SERVICES, LLC,

Defendant.

Lead Case No.: 1:22-cv-01495-ELR

Consolidated with:

Case No.: 1-22-CV-01531-ELR;
Case No.: 1:22-CV-01565-ELR;
Case No.: 1:22-CV-01674-ELR;
Case No.: 1:22-CV-01676-ELR.

JURY TRIAL DEMAND

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Justin Sherwood, Lindsey Quan, Tabatha Bedont, Greg Torrano, Jennifer Hill, Sia Moody, Anthony Ruiz, Alice Dodd, Frederick Lewis, Douglas Ackman, Ryan Evans, Amber Thomas, and Maria Chavez ("Plaintiffs") allege upon personal knowledge as to themselves and their own actions, and upon information and belief, including the investigation of counsel as follows:

I. INTRODUCTION

1. This action arises out of the recent cyberattack and data breach at Horizon Actuarial Services, LLC ("Defendant" or "Horizon") that targeted the

information of consumers and other groups who used Defendant for actuarial services (the "Data Breach").

2. The Data Breach resulted in unauthorized access to the sensitive and confidential data of consumers that used Defendant's services or consumers of financial funds that used Defendant's services. Because of the Data Breach, Plaintiffs and Class Members suffered ascertainable losses inclusive of out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack and the present and substantial continuing risk of imminent harm caused by the compromise of their sensitive personal information, including their names, dates of birth, and Social Security numbers, and health plan information (hereinafter, the "Personally Identifiable Information" or "PII").

3. Defendant's Data Breach occurred on November 10th and 11th of 2021. But Defendant sat on the information for over two months – failing to send data breach consumer notifications until January 13, 2022; and then to individuals nearly two months after that on or about March 9, 2022. When a data set that includes this type of PII is breached, every moment is precious to ensure that that data is not weaponized against the rightful owner through identity theft. Sitting on this information diminished the Data Breach victims' chances at mitigating the consequences resulting from Defendant's failure to provide adequate protection of

the sensitive and private information it chose to maintain for its own financial benefit.

4. As a result of the Data Breach, Plaintiffs and Class Members have been harmed and unnecessarily exposed to a heightened present and continuing risk of fraud and identity theft.

5. Plaintiffs and Class Members have and will continue to incur out-of-pocket costs, for example, through purchasing identity theft protection services, credit freezes, or other protective measures to reasonably deter and detect identity theft for their respective lifetimes. Plaintiffs seek to remedy those harms on behalf of themselves and all similarly situated persons whose PII was unlawfully accessed during the Data Breach. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement for out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual SOC 2 audits, annual assessments by a qualified, independent third-party assessor to ensure that Defendant is complying with the injunctive relief components imposed by the Court, and adequate identity theft services funded by the Defendant.

6. In the notices sent to Plaintiffs and Class Members, Defendant recognized that each Class Member is now subject to the present and continuing risk of identity theft and fraud: Defendant offered Plaintiffs and Class Members identity theft protection from Kroll, who Defendant considers a "fraud specialist." The

offered services for only one year, however, are insufficient to protect Plaintiffs and Class Members from the lifelong implications of having their sensitive PII accessed, acquired, exfiltrated, and/or published on the internet. As another element of damages, Plaintiffs and Class Members seek a sum of money sufficient to provide to Plaintiffs and Class Members identity theft protective services for their respective lifetimes.

7. Consequently, Plaintiffs bring this Action against Defendant seeking redress for its unlawful conduct, asserting claims for: (i) negligence; (ii) negligence *per se*; (iii) unjust enrichment; (iv) declaratory judgment; (v) invasion of privacy; (vi) violations of California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. ("CCPA"), (vii) violations of California's Customer Records Act, Cal. Civ. Code § 1798.81.5; (viii) violations of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*.; (ix) violations of the Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. § 505/1 *et seq*.; (x) violations of the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 598.0915 and NRS 598.0923, *et seq*.; (xi) violations of the Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e)(g) and (u), *et seq*.; (xii) violations of the North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq*.; (xiii) violations of the Idaho Consumer Protection Act, Idaho Code §§ 48-603, *et seq*.; and Idaho Code § 48-603C, *et seq*.; (xiv) violations of Louisiana Database Security Breach Notification

Law, La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.*; (xv) violations of Louisiana Unfair Trade Practices and Consumer Protection Act, La. Rev. Stat. Ann. §§ 51:1401, *et seq.*; and (xvi) violations of the Arkansas Deceptive Trade Practices Act, A.C.A. §§ 4-88-101, *et seq*.

II. JURISDICTION AND VENUE

8. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because Plaintiffs and at least one member of the putative Class, as defined below, are citizens of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

9. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business at 1040 Crown Pointe Parkway, Suite 560, Atlanta, Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendant intentionally availed itself of this jurisdiction by marketing and selling products and services from Georgia to many businesses nationwide.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

III. PARTIES

11. Plaintiff Justin Sherwood is a resident and citizen of Nevada and is a plan participant of an entity that uses Defendant's services. On April 14, 2022, Plaintiff received a "Notice of Data Breach" letter dated April 8, 2022. The letter notified Plaintiff that on November 10 and 11, 2021, two of Defendant's computer servers were accessed by unauthorized actors and that certain PII was included in the files that were accessed including Plaintiff's name, date of birth and Social Security number.

12. Plaintiff Lindsey Quan is a citizen of Oregon, is a plan participant of an entity that uses Defendant's services located in California, where she lived and worked at the time she was associated with that entity, and received the Notice of Data Breach from Defendant dated March 23, 2022 on or about that date.

13. Plaintiff Tabatha Bedont is a resident of Idaho and is a plan participant of an entity that uses Defendant's services. Plaintiff received a "Notice of Data Breach" letter dated March 23, 2022. The letter notified Plaintiff that on November 10 and 11, 2021, two of Defendant's computer servers were accessed by unauthorized actors and that certain PII was included in the files that were accessed, including Plaintiff's name, date of birth and Social Security number.

14. Plaintiff Bedont received the letter under her maiden name Tabatha Johnson. Tabatha Johnson is the name that was provided to Defendant at the time

services were received. Plaintiff Bedont subsequently changed her name to Bedont following her recent marriage.

15. Plaintiff Greg Torrano, is a citizen of California, is a plan participant of an entity that uses Defendant's services, located in Texas where he lived and worked at the time he was associated with that entity, and received the Notice of Data Breach from Defendant dated April 8, 2022 on or about that date.

16. Plaintiff Jennifer Hill is a citizen of Concord, North Carolina residing in Carrabus County, North Carolina. Plaintiff received a Notice of Data Breach letter dated April 13, 2022.

17. Plaintiff Sia Moody is a citizen of Illinois, is a plan participant of an entity that uses Defendant's services, located in Illinois where she lives and worked at the time she was associated with that entity, and received the Notice of Data Breach from Defendant dated May 23, 2022 on or about that date.

18. Plaintiff Anthony Ruiz is a citizen of California, is a plan participant of an entity that uses Defendant's services, and received the Notice of Data Breach from Defendant dated March 23, 2022 on or about that date.

19. Plaintiff Alice Dodd is a citizen of Highland, Arkansas. Plaintiff received a Notice of Data Breach letter dated May 23, 2022.

20. Plaintiff Frederick Lewis is a citizen of New Orleans, Louisiana. Plaintiff received a Notice of Data Breach letter dated May 23, 2022.

21. Plaintiff Douglas Ackman is a citizen of Lake Zurich, Illinois. Plaintiff received a Notice of Data Breach letter dated May 23, 2022.

22. Plaintiff Ryan Evans is a citizen of Ohio, was a plan participant of an entity that uses Defendant's services, and received the Notice of Data Breach from Defendant dated May 6, 2022 on or about that date.

23. Plaintiff Amber Thomas is a citizen of California, was a plan participant of an entity that uses Defendant's services, located in California where she lived and worked at the time she was associated with that entity, and received the Notice of Data Breach from Defendant dated May 20, 2022 on or about that date.

24. Plaintiff Maria Chavez is a citizen of California, was a plan participant of an entity that uses Defendant's services, located in Las Vegas, NV where she lived and worked at the time she was associated with that entity, and received the Notice of Data Breach from Defendant dated April 13, 2022 on or about that date.

25. Defendant Horizon Actuarial Services, LLC is organized under the laws of Delaware and has a principal place of business in Atlanta, Georgia. The members of Horizon as an LLC are the following individuals: (1) Stan Goldfarb, a citizen of Maryland; (2) Mary Ann Dunleavy, a citizen of Maryland; (3) Cary Franklin, a citizen of California; (4) Kathleen Coda, a citizen of California; (5) Ron

Littler, a citizen of California; (6) Mark Lewis, a citizen of Georgia; (7) Nathan Slaff, a citizen of Georgia; and (8) Tom Cliffel, a citizen of Ohio.[1]

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

26. According to the Defendant, it provides actuarial services throughout the United States: Defendant "is a leading consulting firm that specializes in providing innovative actuarial solutions to multiemployer plans."[2]

27. Defendant collects confidential data from business entities that utilize its services about individuals (including Plaintiff and Class Members) to provide its services. That sensitive information includes:

a. Name;

b. Address;

c. Email address;[3]

d. Social Security number; and,

e. Health plan information.[4]

---

[1] *See also* https://www.horizonactuarial.com/about-us.html (noting that Horizon "is an independent company operating as a limited liability corporation incorporated in the state of Delaware. It is owned and operated by its principals.") (last accessed Apr. 17, 2022).
[2] https://www.horizonactuarial.com (last accessed July 7, 2022).
[3] https://www.horizonactuarial.com/website-privacy-policy.html (last accessed July 7, 2022).
[4] HAS's Data Breach Notification, available at https://www.horizonactuarial.com/notice-of-data-incident.html (last accessed July 7, 2022).

28. Defendant's website includes a link titled Notice of Data Incident.[5] The link states that Defendant "is providing notice of a data privacy incident on behalf of itself and the benefit plans listed below to whom Horizon Actuarial provides technical and actuarial consulting services (the 'Plans'). Horizon Actuarial received information regarding plan participants and their family members for business and compliance purposes." Those benefit plans include:

- AFTRA Retirement Fund
- Airconditioning and Refrigeration Industry Health & Welfare Trust Fund
- Airconditioning and Refrigeration Industry Retirement Trust Fund
- Allied Workers Local 48 Pension Plan
- Buffalo Laborers Pension Fund
- Buffalo Laborers Welfare Fund
- California Teachers Assn EE Ret Ben Trust
- Central New York Laborers Pension Fund
- Central Pension Fund of the International Union of Operating Engineers and Participating Employers
- Chauffeurs Teamsters and Helpers Local No. 301 Health and Welfare Fund
- Fox Valley & Vicinity Labor Pension Plan
- Fox Valley & Vicinity Labor Welfare Plan
- Greenville Plumbers Pension Plan
- IBEW 728 Health and Welfare Fund
- IBEW Local 129 Pension Plan
- IBEW Local 1579 Pension Plan
- IBEW Local 540 Pension Plan
- IBEW Local 64 Pension Plan
- Iron Workers Local No. 25 Pension Plan
- IUOE Local Unions 181, 320 & TVA Health & Welfare Trust Fund
- Kansas Building Trades (TW)
- Local 210's Pension Plan
- Major League Baseball Players Benefit Plan
- Massachusetts Bricklayers and Masons Pension Plan
- MCASF Local 725 Pension and Welfare Funds

[5] *Id.*

- National Hockey League Players Association Health and Benefits Fund
- National Roofing Industry Pension Plan
- New York Times Benefit Guild
- OCU Health & Welfare Trust
- OCU Pension Trust
- Operating Engineers Local 324 Pension Plan
- Patriot Retirees Voluntary Employees' Beneficiary Association
- Plumbers Local 630 Pension Plan
- Plumbers Local 630 Welfare Plan
- Retirement Benefit Plan of the Newspaper and Magazine Drivers Chauffeurs and Handlers Union Local 473
- Rocky Mountain UFCW Health Benefit Plan for Retired Employees
- Rocky Mountain UFCW Retail and Meat Pension Plan
- Roofers Local 20 Pension Plan
- Roofers Local No. 20 Health & Welfare Plan
- Roofers Union Local 30 Combined Pension Plan
- SAG - Producers Pension Plan
- San Diego Unified School District and Education Association Joint Employee Welfare Benefits Trust
- Sheet Metal Workers Local Union No. 20 Welfare and Benefit Plan
- Southern Nevada Culinary and Bartenders Pension Fund
- Teamsters 210 Affiliated Pension Fund
- Teamsters Joint Council No. 83 of Virginia Health and Welfare Fund
- Teamsters Joint Council No. 83 of Virginia Pension Fund
- Teamsters Local 1034 Pension Fund
- Teamsters Local 27 Pension Fund
- Teamsters Local 295 Employers Group Welfare Trust
- Teamsters Local 301 Pension Plan
- Teamsters Local 813 Pension Fund
- Twin Cities Bakery Drivers Health & Welfare Fund
- Twin Cities Bakery Drivers Pension Fund
- Twin City Hospital Workers Pension Fund
- UA Local 198 Pension Fund
- UFCW & Employers Benefit Trust
- UFCW 1529 Employers H&W Retiree Fund
- UFCW Comprehensive Benefit Trust
- UFCW Consolidated Pension Fund
- UFCW Intermountain Health Fund, and

- UFCW Local 711 & Retail Food Employers Benefit Fund United Union of Roofers Burial Benefit Fund.[6]

29. Defendant's website confirmed PII was included in the Data Breach: "The investigation revealed that two Horizon Actuarial computer servers were accessed without authorization for a limited period on November 10 and 11, 2021. The group provided a list of information they claimed to have stolen. The types of information impacted may include names, dates of birth, Social Security numbers, and health plan information."[7]

30. In its Privacy Policy, Defendant states that it "respects privacy" and "[w]e use commercially reasonable administrative, technical and organizational measures to help secure Collected Data against loss, misuse, and alteration."[8] Defendant also boasts that it will only share PII "with third parties if we believe it is needed to operate the [website] or to protect our rights or the rights of others, including sharing data needed to identify, contact, or bring legal action."[9]

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

---

[6] *Id.*
[7] *Id.*
[8] https://www.horizonactuarial.com/website-privacy-policy.html (last accessed July 7, 2022).
[9] *Id.*

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

33. Contrary to the Privacy Policy's representation, Defendant failed to respect and protect consumer privacy.

THE DATA BREACH

34. To define data breaches: "a data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed and/or shared without permission."[10]

35. In November of 2021, Defendant experienced a security incident involving unauthorized access to its file servers.

36. Defendant launched an investigation and determined that an unauthorized individual obtained access to files on its storage servers from November 10 to November 11, 2021.

37. Then Defendant sat on the information for over two months – failing to disseminate data breach consumer notifications to the Plans until January 13, 2022; and then to individuals nearly two months later on or about March 9, 2022. Since the initial notice to impacted customers, Defendant notified various Attorneys General of even more impacted persons, as late as June 9, 2022. These later

[10] "*How Data Breaches Happen*," KASPERSKY, at https://www.kaspersky.com/resource-center/definitions/data-breach (last accessed July 7, 2022).

identified persons referred to in these notices were not notified that they were impacted by the Data Breach for as long as six months.

38. The sensitive PII stolen in the Data Breach included Class Members' names, dates of birth, Social Security number, and, for some, health plan information.

39. The PII contained in the files accessed in the Data Breach was not encrypted or redacted.

40. Plaintiffs and Class Members provided their PII to Defendant with the reasonable expectation and the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the breach.

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

SECURING PII AND PREVENTING DATA BREACHES

42. Defendant could have prevented this Data Breach by properly encrypting or otherwise protecting its equipment and computer files containing PII, but did not do so.

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

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

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

45. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[11]

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

47. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the

[11] *See* https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed July 7, 2022).

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

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

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

50. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private

and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

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

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

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

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

a. Maintaining a secure firewall configuration;

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

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

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

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs;

j. Monitoring for server requests from Tor exit nodes;

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

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

54. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

[12] 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number."[13]

55. The ramifications of Defendant's failure to keep its consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims is likely to continue for years.

THE VALUE OF PERSONALLY IDENTIFIABLE INFORMATION

56. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[15]

---

[13] *Id*.

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 7, 2022).

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

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

58. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

59. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, 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

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 7, 2022).

obtain a new number.

60. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

61. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[18]

62. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[19]

63. Given the nature of Defendant's Data Breach, as well as the length of

---

[17] 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 (last accessed July 7, 2022).

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 7, 2022).

[19] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

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

64. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[20] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

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

66. The injuries to Plaintiffs and Class Members were directly and

[20] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed July 7, 2022).

proximately caused by Defendant's failure to implement or maintain adequate data security measures.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

67. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision- making.

68. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[21] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data

[21] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016), *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 7, 2022).

being transmitted from the system; and have a response plan ready in the event of a breach.[22]

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

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

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

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

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

[22] *Id.*

74. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

75. Other best cybersecurity practices that are standard in the Defendant's industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

76. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

DEFENDANT'S BREACH

78. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect consumers' PII;

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

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

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

f. Failing to adhere to industry standards for cybersecurity.

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

80. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members lost the benefit of the bargain they made with Defendant.

HARM TO CONSUMERS

81. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

82. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

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

84. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it

possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

85. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

86. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23] The fraudulent activity resulting from the Data Breach may not come to light for years.

87. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

88. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members,

[23] 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 (last accessed July 7, 2022).

including Social Security numbers and driver's license numbers, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

89. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

HARM TO PLAINTIFFS

Plaintiff Justin Sherwood (Nevada)

90. On or about April 13, 2022, Plaintiff Justin Sherwood received notice from Defendant that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Sherwood's PII, including his name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

91. As a result of the Data Breach, Plaintiff Sherwood made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit card and financial account statements for any indications of actual or attempted identity theft or fraud and he has monitored his Credit Karma account extensively since receiving the Notice of Data Incident

from Defendant. Plaintiff Sherwood intends to spend additional time taking steps to protect his PII. Plaintiff Sherwood has spent approximately 2-3 hours dealing with the Data Breach, valuable time Plaintiff Sherwood otherwise would have spent on other activities, including but not limited to work and/or recreation.

92. As a result of the Data Breach, Plaintiff Sherwood has experienced anger and frustration as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including worry about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Sherwood is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

93. Plaintiff Sherwood suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Sherwood; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

94. Plaintiff Sherwood has also experienced a substantial number of suspicious and "spam" telephone calls and texts since the Data Breach. Plaintiff

Sherwood believes these suspicious telephone calls and texts may be a result of the Data Breach.

95. As a result of the Data Breach, Plaintiff Sherwood anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Sherwood is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Lindsey Quan (Oregon)

96. On or about May 23, 2022, Plaintiff Lindsey Quan received notice from Defendant that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Quan's PII, including her name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

97. As a result of the Data Breach, Plaintiff Quan made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services. Plaintiff Quan has also had to freeze her credit in order to prevent any unauthorized use of her social security number, disclosed by Defendant in the Data Breach. Plaintiff Quan has spent at least

3 hours dealing with the Data Breach, valuable time Plaintiff Quan otherwise would have spent on other activities, including but not limited to work and/or recreation.

98. As a result of the Data Breach, Plaintiff Quan has suffered anxiety as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Quan is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

99. Plaintiff Quan suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Quan; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

100. Plaintiff Quan has also experienced a substantial increase in suspicious and "spam" telephone calls and emails since the Data Breach. These suspicious telephone calls and emails are of a different character than those she had previously received. Plaintiff Quan believes these suspicious telephone calls and emails to be a result of the Data Breach.

101. As a result of the Data Breach, Plaintiff Quan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address

harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Quan is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Tabatha Bedont (Idaho)

102. Plaintiff Bedont typically takes measures to protect her PII and is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

103. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She monitors accounts and credit scores and has sustained emotional distress as a result of worrying about her PII being exfiltrated. She has also monitored her credit account extensively since receiving the Notice of Data Incident from Defendant and intends to spend time taking steps to protect her PII. This is time that was and will be lost and unproductive and taken away from other activities and duties.

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

105. As a result of the Data Breach, Plaintiff Bedont has suffered anxiety as a result of the release of her PII, which she believed would be protected from

unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Bedont is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

106. Plaintiff Bedont suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Bedont; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

107. As a result of the Data Breach and the exfiltration of her unencrypted PII in the hands of criminals, Plaintiff is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

Plaintiff Greg Torrano (California)

108. On or about April 8, 2022, Plaintiff Greg Torrano received notice from Defendant that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Torrano's PII, including his name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

109. As a result of the Data Breach, Plaintiff Torrano made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to:

researching the Data Breach; reviewing credit card and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Torrano has spent approximately 2-3 hours dealing with the Data Breach, valuable time Plaintiff Torrano otherwise would have spent on other activities, including but not limited to work and/or recreation.

110. As a result of the Data Breach, Plaintiff Torrano has experienced anger and frustration as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including worry about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Torrano is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

111. Plaintiff Torrano suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Torrano; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

112. Plaintiff Torrano has also experienced a substantial increase in suspicious and "spam" telephone calls and texts since the Data Breach. These

suspicious telephone calls and texts are of a different character than those he had previously received, being targeted towards him based on his Medicare status, insurance, and funeral services, among others. Plaintiff Torrano believes these suspicious telephone calls and texts to be a result of the Data Breach.

113. As a result of the Data Breach, Plaintiff Torrano anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Torrano is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Jennifer Hill (North Carolina)

114. On or about April 13, 2022, Plaintiff Jennifer Hill received notice from Defendant that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Hill's PII, including her name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

115. As a result of the Data Breach, Plaintiff Hill suffered a fraudulent charge on her credit card for approximately $50. Plaintiff, in turn, was required to contact her bank, remove the charge as fraudulent, and cancel her credit card account.

116. As a result of the Data Breach, Plaintiff Hill made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services. Plaintiff Hill has spent 3 hours dealing with the Data Breach, valuable time Plaintiff Hill otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

117. As a result of the Data Breach, Plaintiff Hill has suffered anxiety as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Hill is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

118. Plaintiff Hill suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Hill; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

119. Plaintiff Hill has also experienced a substantial increase in suspicious and "spam" telephone calls and texts since the Data Breach. These suspicious

telephone calls and texts increased in frequency around the time of the Data Breach relative to those that she had previously received. Plaintiff Hill believes these suspicious telephone calls and texts to be a result of the Data Breach.

120. As a result of the Data Breach, Plaintiff Hill anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Hill is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Sia Moody (Illinois)

121. On or about May 23, 2022, Plaintiff Sia Moody received notice from Defendant that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Moody's PII, including her name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

122. As a result of the Data Breach, Plaintiff Moody made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Moody has spent approximately 40 hours dealing with the Data Breach, valuable

time Plaintiff Moody otherwise would have spent on other activities, including but not limited to work and/or recreation.

123. As a result of the Data Breach, Plaintiff Moody has suffered stress and anxiety as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Moody is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

124. Plaintiff Moody suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Moody; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

125. Plaintiff Moody has also experienced a substantial increase in suspicious and "spam" telephone calls, text messages, and emails since the Data Breach. These suspicious telephone calls, text messages, and emails are of a different character than those she had previously received. Plaintiff Moody believes these suspicious telephone calls, text messages, and emails to be a result of the Data Breach.

126. In July of 2022, Plaintiff Moody learned that an unauthorized email account was linked to her Chase Visa credit card. The email account belongs to an unknown individual named "Frank." Shortly after the Data Breach, Plaintiff Moody began receiving a lot of spam emails addressed to an individual named "Frank." Plaintiff Moody intends to cancel her credit card and obtain a new one.

127. As a result of the Data Breach, Plaintiff Moody anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Moody is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Doug Ackman (Illinois)

128. On or about May 23, 2022, Plaintiff Ackman received a notice from Defendant that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Ackman's PII, including his name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

129. As a result of the Data Breach, Plaintiff Ackman was notified that his PII is now exposed on the dark web.

130. As a result of the Data Breach, Plaintiff Ackman incurred $200 in out-of-pocket costs for an identity theft protection program subscription known as Identity Force.

131. Plaintiff Ackman purchased Identity Force in direct response to the Data Breach caused by Defendant's negligence.

132. Plaintiff Ackman purchased Identity Force because he did not believe Defendant's offer of credit monitoring was sufficient to protect his PII.

133. As a result of the Data Breach, Plaintiff Ackman instituted a credit freeze to further protect his PII.

134. As a result of the Data Breach, Plaintiff Ackman made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services. Plaintiff Ackman has spent approximately 10 hours dealing with the Data Breach, valuable time Plaintiff Ackman otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

135. As a result of the Data Breach, Plaintiff Ackman has suffered anxiety as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties

viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Ackman is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

136. Plaintiff Ackman suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Ackman; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

137. Plaintiff Ackman has also experienced a substantial increase in suspicious and "spam" telephone calls and emails since the Data Breach. These suspicious telephone calls and emails are of a different character than those he had previously received. Plaintiff Ackman believes these suspicious telephone calls and emails to be a result of the Data Breach.

138. As a result of the Data Breach, Plaintiff Ackman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Ackman is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Anthony Ruiz (California)

139. On or about March 23, 2022, Plaintiff Anthony Ruiz received notice from Defendant that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Ruiz's PII, including his name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

140. As a result of the Data Breach, Plaintiff Ruiz made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Defendant; paying an initial $30 fee for Experian credit monitoring services and a monthly fee of the same. Plaintiff Ruiz has spent several hours dealing with the Data Breach, valuable time Plaintiff Ruiz otherwise would have spent on other activities, including but not limited to work and/or recreation.

141. Recently, Plaintiff Ruiz has had multiple inquiries made on his credit reports for loans for which he did not submit applications, that he reasonably believes are a result of the Data Breach.

142. As a result of the Data Breach, Plaintiff Ruiz has suffered anxiety as a result of the release of his PII, which he believed would be protected from

unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Ruiz is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

143. Plaintiff Ruiz suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Ruiz; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

144. As a result of the Data Breach, Plaintiff Ruiz anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Ruiz is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Alice Dodd (Arkansas)

145. Plaintiff Dodd received a notice from Defendant that her PII had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Dodd's PII, including her name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

146. As a result of the Data Breach, Plaintiff Dodd suffered a fraudulent tax return filed on her behalf. Plaintiff Dodd, in turn, suffered harm from her identity theft and extensive invasion into her privacy.

147. As a result of the Data Breach, Plaintiff Dodd purchased her own identity theft protection program to guard against future harm resulting from the data breach. Because Plaintiff Dodd was required to purchase her own identity theft protection program, Plaintiff Dodd suffered monetary loss of $15 per month due to the Data Breach.

148. As a result of the Data Breach, Plaintiff Dodd made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services. Plaintiff Dodd and/or her power of attorney spent several hours dealing with the Data Breach, valuable time Plaintiff Dodd otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

149. As a result of the Data Breach, Plaintiff Dodd has suffered anxiety as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud.

Plaintiff Dodd is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

150. Plaintiff Dodd suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Dodd; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

151. As a result of the Data Breach, Plaintiff Dodd anticipates spending time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Dodd is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Frederick Lewis (Louisiana)

152. On or about May 23, 2022, Plaintiff Lewis received a notice from Defendant that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Lewis' PII, including his name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

153. As a result of the Data Breach, Plaintiff Lewis suffered a fraudulent charge on his personal credit card. Plaintiff Lewis, in turn, was required to contact his bank, remove the charge as fraudulent, and cancel and replace his credit card.

154. As a result of the Data Breach, Plaintiff Lewis was notified that his PII is now exposed on the dark web.

155. As a result of the Data Breach, Plaintiff Lewis made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services. Plaintiff Lewis has spent 3 hours dealing with the Data Breach, valuable time Plaintiff Lewis otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

156. As a result of the Data Breach, Plaintiff Lewis has suffered anxiety as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Lewis is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

157. Plaintiff Lewis suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Lewis; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

158. Plaintiff Lewis has also experienced a substantial increase in suspicious and "spam" telephone calls and emails since the Data Breach. These suspicious telephone calls and emails are of a different character than those he had previously received. Plaintiff Lewis believes these suspicious telephone calls and emails to be a result of the Data Breach.

159. As a result of the Data Breach, Plaintiff Lewis anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Lewis is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Ryan Evans (Ohio)

160. On or about May 6, 2022, Plaintiff Ryan Evans received notice from Defendant that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Evans's PII, including his name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

161. As a result of the Data Breach, Plaintiff Evans made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit

monitoring and identity theft protection services offered by Defendant. Plaintiff Evans has also had to freeze his credit in order to prevent any unauthorized use of his social security number, disclosed by Defendant in the Data Breach. Plaintiff Evans has spent eight hours dealing with the Data Breach, valuable time Plaintiff Evans otherwise would have spent on other activities, including but not limited to work and/or recreation.

162. As a result of the Data Breach, Plaintiff Evans has suffered anxiety as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Evans is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

163. Plaintiff Evans suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Evans; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

164. Plaintiff Evans has suffered additional actual injury in the form of someone using his information to attempt to open a new bank account in his name

in June 2022. Plaintiff Evans has had to spend time contacting his bank to correct this fraudulent transaction and confirm the account has been closed.

165. Plaintiff Evans has also experienced a substantial increase in suspicious and "spam" telephone calls and emails since the Data Breach. These suspicious telephone calls and emails are of a different character than those he had previously received. Plaintiff Evans believes these suspicious telephone calls and emails to be a result of the Data Breach.

166. As a result of the Data Breach, Plaintiff Evans anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Evans is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Amber Thomas (California)

167. On or about May 20, 2022, Plaintiff Amber Thomas received notice from Defendant that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Thomas's PII, including her name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

168. As a result of the Data Breach, Plaintiff Thomas made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to:

researching the Data Breach and researching a billing issue with the Screen Actors Guild ("SAG"), a client of Defendant. Plaintiff Thomas spent about a week dealing with the Data Breach, valuable time Plaintiff Thomas otherwise would have spent on other activities, including but not limited to work and/or recreation.

169. As a result of the Data Breach, Plaintiff Thomas has suffered anxiety as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Thomas is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

170. Plaintiff Thomas suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Thomas; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

171. Plaintiff Thomas has also experienced a substantial increase in suspicious and "spam" telephone calls since the Data Breach. Plaintiff Thomas believes these suspicious telephone calls to be a result of the Data Breach.

172. As a result of the Data Breach, Plaintiff Thomas anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address

harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Thomas is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Maria Chavez (California)

173. On or about April 13, 2022, Plaintiff Maria Chavez received notice from Defendant that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Chavez's PII, including her name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

174. As a result of the Data Breach, Plaintiff Chavez made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach and checking for fraudulent activity on her accounts. Plaintiff Chavez has spent about a 40 Hours dealing with the Data Breach, valuable time Plaintiff Chavez otherwise would have spent on other activities, including but not limited to work and/or recreation.

175. As a result of the Data Breach, Plaintiff Chavez has suffered anxiety as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud.

Plaintiff Chavez is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

176. Plaintiff Chavez suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Chavez; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

177. As a result of the Data Breach, Plaintiff Chavez anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Chavez is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

178. As a result of the Data Breach, Plaintiff Chavez has lost access to her pension fund and has been unable to receive payments for 4 months.

V. CHOICE OF LAW ANALYSIS

179. The state of Georgia has a significant interest in regulating the conduct of businesses operating within its borders. Georgia, which seeks to protect the rights and interests of Georgia and all residents and citizens of the United States against a company headquartered and doing business in Georgia, has a greater interest in the

nationwide claims of Plaintiffs and Nationwide Class members than any other state, and is most intimately concerned with the claims and outcome of this litigation.

180. The principal place of business of Defendant, located at 1040 Crown Pointe Parkway, Suite 560, Atlanta, Georgia, is the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security functions and major policy, financial, and legal decisions.

181. Defendant's response to the data breach at issue here, and corporate decisions surrounding such response, were made from and in Georgia.

182. Defendant's breaches of duty to Plaintiffs and Nationwide Class members emanated from Georgia.

183. Application of Georgia law to the Nationwide Class with respect to Plaintiffs' and Class members' common law claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Nationwide Class.

184. Under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia applies to the nationwide common law claims of all Nationwide Class members.

VI. CLASS ALLEGATIONS

185. Plaintiffs bring this Action on behalf of themselves and on behalf of all other persons similarly situated. Plaintiffs propose the following Class and Subclass definitions, subject to amendment as appropriate:

All natural persons residing in the United States whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "Nationwide Class" or "Class");

All natural persons residing in Arkansas whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "Arkansas Class" or "Arkansas Subclass");

All natural persons residing in California whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "California Class" or "California Subclass");

All natural persons residing in Idaho whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "Idaho Class" or "Idaho Subclass");

All natural persons residing in Illinois whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "Illinois Class" or "Illinois Subclass");

All natural persons residing in Louisiana whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "Louisiana Class" or "Louisiana Subclass");

All natural persons residing in Nevada whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "Nevada Class" or "Nevada Subclass");

All natural persons residing in North Carolina whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "North Carolina Class" or "North Carolina Subclass"); and,

All natural persons residing in Oregon whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "Oregon Class" or "Oregon Subclass").

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

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

188. **Commonality**. There are questions of law and fact common to the Class and Subclasses, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether the Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to, during, and after the Data Breach complied with the applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached a duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members PII in the Data Breach;

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

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

j. Whether Defendant's conduct was negligent;

k. Whether the Defendant's conduct violated the Arkansas Deceptive Trade Practices Act;

l. Whether the Defendant's conduct violated California's Consumer Privacy Act;

m. Whether the Defendant's conduct violated the California's Customer Records Act;

n. Whether the Defendant's conduct violated California's Unfair Competition Law;

o. Whether the Defendant's conduct violated the Idaho Consumer Protection Act;

p. Whether the Defendant's conduct violated the Illinois Consumer Fraud Act;

q. Whether the Defendant's conduct violated the Louisiana Database Security Breach Notification Law;

r. Whether the Defendant's conduct violated the Louisiana Unfair Trade Practices and Consumer Protection Law;

s. Whether the Defendant's conduct violated the Nevada Deceptive Trade Practices Act;

t. Whether the Defendant's conduct violated the North Carolina Unfair Deceptive Trade Practices Act;

u. Whether the Defendant's conduct violated the Oregon Unfair Trade Practices Act;

v. Whether Defendant failed to provide notice of the Data Breach in a timely manner in violation of the relevant state consumer protection and data breach notice statutes;

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

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

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

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

192. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

193. Defendant has acted on grounds that apply generally to the Classes as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

VII. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

194. Plaintiffs and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

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

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

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

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

199. Defendant owed a common law duty to Plaintiffs and the Class to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This common law duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and Class Members' information in Defendant's possession was adequately secured and protected.

200. Defendant's common law duty it owed to Plaintiffs and the Class included the duty to exercise appropriate clearinghouse practices to remove PII

belonging to persons who transacted with its former customers that Defendant was no longer required to retain pursuant to regulations.

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

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

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

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

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

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

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

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

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

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

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

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

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

213. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiffs and the Class by failing to implement at a very minimum the

standard industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Class when the PII was within Defendant's possession or control.

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

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

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

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

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

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

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

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

subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Plaintiffs' and Class Members' PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members.

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

223. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

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

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

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class)

226. Plaintiffs and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

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

228. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendant's duty in this regard.

229. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

230. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the

foreseeable consequences of the damages that would result to Plaintiffs and the Class.

231. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

232. Plaintiffs and the Class are within the class of persons that Section 5 of the FTC Act was intended to protect.

233. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

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

tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Plaintiffs' and Class Members' PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members.

235. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

236. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

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

238. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

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

239. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

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

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

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

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

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

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

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

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

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

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

COUNT IV
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Nationwide Class)

250. Plaintiffs and Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

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

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

253. Defendant owes duties of care to Plaintiffs and Nationwide Class Members which require them to adequately secure their PII.

254. Defendant still possesses Plaintiffs' and Nationwide Class Members' PII.

255. Defendant does not specify in the *Notice of Data Breach* letter what steps they have taken to prevent this from occurring again.

256. Plaintiffs and Nationwide Class Members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

257. An actual controversy has arisen in the wake of the Defendant Data Breach regarding its present and prospective common law and other duties to reasonably safeguard Plaintiffs' and the Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their PII.

258. Plaintiffs and the Class, therefore, seek a declaration that (1) each of Defendant's existing security measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect consumers' personal information, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging 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;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting 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;

g. Purchasing credit monitoring services for Plaintiffs and Nationwide Class Members for a period of ten years;

h. Meaningfully educating Plaintiffs and Nationwide Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and

i. The appointment of a qualified and independent third party assessor, funded by Defendant, who shall be charged with assessing

Defendant's compliance with the injunctive components of the relief imposed by the court, and who shall distribute to counsel for the Class on an annual basis a report reflecting the details of the assessor's assessment.

259. The Court should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with the law and industry standards to protect Plaintiffs' and Class Members' PII.

260. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach by Defendant. The risk of another data breach is real, immediate, and substantial.

261. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs at Horizon, Plaintiffs and the Class will likely be subjected to fraud, identity theft, and other harms described herein. But, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is minimal given it had pre-existing legal obligations to employ these measures.

COUNT V
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class)

262. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

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

264. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

265. Defendant owed a duty to Plaintiffs and Class Members to keep their PII contained as a part thereof, confidential.

266. Defendant failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII of Plaintiffs and Class Members.

267. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and Class Members, by way of Defendant's failure to protect the PII.

268. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members is highly offensive to a reasonable person.

269. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Defendant as part of their relationships with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

270. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

271. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

272. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

273. Moreover, Defendant also has a duty under the Georgia Constitution ('the Constitution') which contains a Right to Privacy clause, Chapter 1, Article 1, to protect its users' private information. The Georgia Constitution states "no person shall be deprived of life, liberty, or property except by due process of law."

Moreover, the Georgia Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

274. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) §652A which specifically recognized four common law invasion of privacy claims in Georgia, which include 1) appropriation of likeness; 2) intrusion on solitude or seclusion; 3) public disclosure of private facts; and 4) false light.

275. Defendant's implementation of inadequate data security measures and its abdication of its responsibility to reasonably protect data it required Plaintiffs and the Class to provide and stored on its own servers and databases constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

276. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

277. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class

Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

COUNT VI
VIOLATION OF ARKANSAS DECEPTIVE TRADE PRACTICES ACT
(On Behalf of Plaintiff Dodd and the Arkansas Subclass)

278. Plaintiff Dodd ("Plaintiff," for purposes of this Count), individually and on behalf of the Arkansas Subclass, re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 178.

279. Defendant is a "person" as defined by A.C.A. § 4-88-102(5).

280. Defendant's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

281. Defendant advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

282. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101, et seq., prohibits unfair, deceptive, false, and unconscionable trade practices.

283. Defendant engaged in unconscionable, false, and deceptive acts and practices including by:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arkansas Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 the GLBA, 15 U.S.C. § 6801, et seq., and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Arkansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, et seq., and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arkansas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq*., and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b).

284. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

285. Defendant intended to mislead Plaintiff and Arkansas Subclass members and induce them to rely on its misrepresentations and omissions.

286. Had Defendant disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself out as having a special role in the financial system with a corresponding duty of trustworthiness and care, Plaintiff and the Arkansas Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

287. Defendant acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Arkansas Subclass members' rights.

288. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts or practices and Plaintiff Dodd's and Arkansas Subclass members' reliance thereon, Plaintiff and Arkansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time

and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

289. Plaintiff and the Arkansas Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

COUNT VII
VIOLATION OF CALIFORNIA'S CONSUMER PRIVACY ACT
(On Behalf of Plaintiffs Chavez, Ruiz, and Thomas and the California Subclass)

290. Plaintiffs Chavez, Ruiz, and Thomas ("California Plaintiffs") and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

291. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent California Plaintiffs' and the California Subclass's nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiffs and the California Subclass.

292. As a direct and proximate result of Defendant's acts, California Plaintiffs' and the California Class's PII was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendant's computer network.

293. As a direct and proximate result of Defendant's acts, California Plaintiffs and the California Subclass were injured and lost money or property, including but not limited to the loss of the California Subclass's legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

294. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass's PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of California Plaintiffs and the California Class.

295. Defendant is organized or operated for the profit or financial benefit of its shareholders. Defendant collected California Plaintiffs' and the California Class's PII as defined in Cal. Civ. Code § 1798.140.

296. On information and belief, Defendant (a) has a gross annual revenue of over $25 million and (b) buys, receives, or sells the personal information of 50,000 or more California residents, households, or devices.

297. Pursuant to Section 1798.150(b) of the CCPA, Plaintiffs Chavez, Ruiz and Thomas have given written notice to Defendant of its specific violations of section 1798.150(a) by a certified mail letter. Defendant timely responded to these Plaintiffs' CCPA notices but failed to "actually cure" the violations by, among other things, not effectively retrieving and securing the lost data, not encrypting Plaintiffs' PII and the California Subclass's PII that remained on its systems, and by not deleting data it no longer had a reasonable need to maintain in an Internet accessible environment. Defendant claims it retrieved and secured the lost data by paying a ransom to cybercriminals in exchange for an "agreement" that the criminals would "delete and not distribute or otherwise misuse" Plaintiffs' and the Class's sensitive PII.

298. Thus, Defendant has failed to "actually cure" its violations within 30 days of the written notice.

299. As a result, California Plaintiffs and the California Subclass seek relief under § 1798.150(a), including, but not limited to, statutory damages in an amount not less than one hundred fifty dollars ($150) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater; injunctive or declaratory relief; any other relief the Court deems proper; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

COUNT VIII
VIOLATION OF CALIFORNIA'S CUSTOMER RECORDS ACT
(On Behalf of Plaintiffs Chavez, Ruiz, Thomas and Torrano and the California Subclass)

300. California Plaintiffs Chavez, Ruiz, Thomas and Torrano and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

301. This Count is brought on behalf of California Plaintiffs and the California Subclass.

302. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

303. Defendant is a business that maintains PII about California Plaintiffs and California Subclass Members within the meaning of Cal. Civ. Code § 1798.81.5. Such PII includes, but is not limited to, the first and last names of California Plaintiffs and the California Subclass Members, along with account numbers or credit or debit card numbers, in combination with any required security code, access

code, or password that would permit access to California Plaintiffs and the California Subclass Members' financial accounts. *See* Cal. Civ. Code § 1798.81.5(d)(1)(A)(iii).

304. Businesses that maintain computerized data that includes PII are required to "notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b). Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

305. Defendant is a business that maintains computerized data that includes PII as defined by Cal. Civ. Code § 1798.80.

306. California Plaintiffs and California Subclass Members' PII includes Personal Information as covered by Cal. Civ. Code § 1798.82.

307. Because Defendant reasonably believed that California Plaintiffs and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach, immediately following its discovery, to the owners or licensees of the PII (i.e., California Plaintiffs and the California Subclass Members) as mandated by Cal. Civ. Code § 1798.82.

308. By failing to disclose the Data Breach immediately following its discovery, Defendant violated Cal. Civ. Code § 1798.82.

309. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, California Plaintiffs and California Subclass Members suffered damages, as described above and as will be proven at trial.

310. California Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT IX
VIOLATION OF THE UNLAWFUL AND UNFAIR PRONG OF CALIFORNIA'S UNFAIR COMPETITION LAW
(On Behalf of Plaintiffs Chavez, Ruiz, Thomas and Torrano and the California Subclass)

311. California Plaintiffs Chavez, Ruiz, Thomas and Torrano and the California Subclass, re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

312. Defendant engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting California Plaintiffs' and the Nationwide Class's PII with knowledge that the information would not be adequately protected; and by storing California Plaintiffs' and the California Class's PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous,

unconscionable, and/or substantially injurious to California Plaintiffs and the California Class. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiffs and the California Class outweighed their utility, if any.

313. Defendant engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and security measures and protect California Plaintiffs' and the California Class's PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and the California Class. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiffs and the Nationwide Class outweighed their utility, if any.

314. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiffs and the California Class were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Plaintiffs' and the California Class's legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

315. Defendant also violated Cal. Bus. And Prof. Code § 17200, et seq., by engaging in unlawful, business acts and practices that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

316. Defendant engaged in unlawful acts and practices with respect to its services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and the Class's PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and the Class's PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiffs and the Nationwide Class. Defendant also violated: the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, et seq. and the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, et seq.; and also the California Financial Information Privacy Act, California Financial Code § 4052.5; the Graham Leach Bliley Act Privacy Rule, 16 C.F.R. Part 313, and Reg. P, 12 C.F.R. Part 1016; and Article 1, § 1 of the California Constitution.

317. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the data breach to the Class in a timely and accurate manner, contrary to

the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendant still has not provided such information to California Plaintiffs and the Nationwide Class.

318. As a direct and proximate result of Defendant's unlawful practices and acts, California Plaintiffs and the Class were injured and lost money or property, including, but not limited to, the price received by Defendant for the services, the loss of the Class's legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

319. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and the Class's PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of California Plaintiffs and the Class.

320. California Plaintiffs and the California Subclass seek relief under Cal. Bus. & Prof. Code § 17200, et seq., including, but not limited to, restitution to California Plaintiffs and the California Subclass of money or property that the Defendant may have acquired by means of its unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

COUNT X
VIOLATION OF IDAHO'S CONSUMER PROTECTION ACT
(On Behalf of Plaintiff Bedont and the Idaho Subclass)

321. Plaintiff Bedont ("Plaintiff," for purposes of this Count) and the Idaho Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

322. Plaintiff Bedont brings this Count on her own behalf and that of the Idaho Subclass for violations of the Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), et seq.; and Idaho Code § 48-603C, et seq.

323. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale, performance, and advertisement of its services, including: (1) failing to maintain adequate data security to keep Plaintiff Bedont's and the Idaho Subclass's sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff Bedont and the Idaho Subclass regarding its lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff Bedont and the Idaho Subclass; (3) failing to disclose or omitting materials facts to Plaintiff Bedont and the Idaho Subclass about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and

security of the PII of Plaintiff Bedont and the Idaho Subclass; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Bedont and the Idaho Subclass's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

324. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff Bedont and the Idaho Subclass and defeat their reasonable expectations about the security of their PII.

325. Moreover, Defendant represented that it would maintain the data it collected and custodied in a secure manner and endeavor to keep it safe from unauthorized access and exfiltration.

326. Defendant intended that Plaintiff Bedont and the Idaho Subclass rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

327. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Idaho Subclass. Plaintiff Bedont and the Idaho Subclass have been

adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

328. Defendant also violated Idaho Code Ann. § 28-51-105(1), et seq., by failing to immediately notify Plaintiff Bedont and the Idaho Subclass of the nature and extent of the Data Breach.

329. As a result of Defendant's wrongful conduct, Plaintiff Bedont and the Idaho Subclass were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

330. As a direct and proximate result of Defendant's violations described herein, Plaintiff Bedont and the Idaho Subclass have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiff Bedont and the Idaho Subclass would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use

or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

331. Plaintiff Bedont and the Idaho Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of Idaho's consumer protection statutes.

COUNT XI
VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT
(On Behalf of Plaintiff Moody, Ackman, and the Illinois Subclass)

332. Plaintiffs Moody, Ackman, and the Illinois Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

333. Plaintiffs Moody, Ackman, and the Illinois Subclass are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiffs Moody, Ackman, the Illinois Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

334. Defendant is engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

335. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of its services in violation of the CFA, including: (1)

failing to maintain adequate data security to keep Plaintiff Moody's, Plaintiff Ackman's and the Illinois Subclass's sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiffs Moody, Ackman, and the Illinois Subclass regarding its lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiffs Moody, Ackman, and the Illinois Subclass; (3) failing to disclose or omitting materials facts to Plaintiffs Moody, Ackman, and the Illinois Subclass about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiffs Moody, Ackman, and the Illinois Subclass; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Moody's, Plaintiff Ackman's, and the Illinois Subclass's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

336. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiffs Moody, Ackman, and the

Illinois Subclass and defeat their reasonable expectations about the security of their PII.

337. Moreover, Defendant represented that it would maintain the data it collected and custodied in a secure manner and endeavor to keep it safe from unauthorized access and exfiltration.

338. Defendant intended that Plaintiffs Moody, Ackman, and the Illinois Subclass rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

339. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Illinois Subclass. Plaintiffs Moody, Ackman, and the Illinois Subclass have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

340. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs Moody, Ackman, and the Illinois Subclass of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, et seq.

341. As a result of Defendant's wrongful conduct, Plaintiffs Moody, Ackman, and the Illinois Subclass were injured in that they never would have

provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

342. As a direct and proximate result of Defendant's violations of the CFA, Plaintiffs Moody, Ackman, and the Illinois Subclass have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiffs Moody, Ackman, and the Illinois Subclass would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

343. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiffs Moody, Ackman, and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

COUNT XII
VIOLATION OF LOUISIANA'S DATABASE SECURITY BREACH NOTIFICATION LAW
(On Behalf of Plaintiff Lewis and the Louisiana Class)

344. Plaintiff Lewis ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and re-alleges Paragraphs 1-178 as if fully alleged herein.

345. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by La. Rev. Stat. Ann. § 51:3074(C).

346. Plaintiff's and Louisiana Subclass members' Personal Information (e.g., Social Security numbers) includes Personal Information as covered under La. Rev. Stat. Ann. § 51:3074(C).

347. Defendant is required to accurately notify Plaintiff and Louisiana Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

348. Because Defendant was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information, Defendant had an obligation to

disclose the Horizon data breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

349. By failing to disclose the Horizon data breach in a timely and accurate manner, Defendant violated La. Rev. Stat. Ann. § 51:3074(C).

350. As a direct and proximate result of Defendant's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass members suffered damages, as described above.

351. Plaintiff and Louisiana Subclass members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

COUNT XIII
VIOLATION OF LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
(On Behalf of Plaintiff Lewis and the Louisiana Subclass)

352. Plaintiff Lewis ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and re-alleges Paragraphs 1-178 as if fully alleged herein.

353. Defendant, Plaintiff, and the Louisiana Subclass members are "persons" within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

354. Plaintiff and Louisiana Subclass members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

355. Defendant engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

356. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

357. Defendant participated in unfair and deceptive acts and practices that violated the Louisiana CPL, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Louisiana Subclass members' Personal Information, which was a direct and proximate cause of the Horizon data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Horizon data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the

FTC Act, 15 U.S.C. § 45 and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Horizon data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Louisiana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the GLBA, 15 U.S.C. § 6801, et seq.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Louisiana Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the GLBA, 15 U.S.C. § 6801, *et seq*.

358. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

359. Defendant intended to mislead Plaintiff and Louisiana Subclass members and induce them to rely on its misrepresentations and omissions.

360. Defendant's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Louisiana Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

361. Defendant acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Louisiana Subclass members' rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

362. Had Defendant disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself

out as having a special role in the financial system with a corresponding duty of trustworthiness and care, Plaintiff and the Louisiana Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

363. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Louisiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

364. Plaintiff and Louisiana Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Defendant's knowing violations of the Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper

COUNT XIV
VIOLATION OF NEVADA'S DECEPTIVE TRADE PRACTICES ACT
(On Behalf of Plaintiff Sherwood and the Nevada Subclass)

365. Plaintiff Sherwood ("Plaintiff," for purposes of this Count) and the Nevada Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

366. This Count is brought on behalf of Plaintiff Sherwood and the Nevada Subclass.

367. In the course of its businesses, Defendant engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to its employment and/or business affiliation with persons in the State of Nevada in violation of Nev. Rev. Stat. § 598.0915 and NRS 598.0923(3), including but not limited to the following:

a. Defendant misrepresented material facts, pertaining to the storing of Plaintiff's Personal Data, to the Nevada Subclass by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Nevada Subclass Members' Personal Data from unauthorized disclosure, release, data breaches, and theft, in violation of Nev. Rev. Stat. § 598.0915(15);

b. Defendant misrepresented material facts, pertaining to the storage of the personal data belonging to the Nevada Subclass by representing by implication that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nevada Class Members' Personal Data, in violation of Nev. Rev. Stat. § 598.0915(15);

c. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Nevada Subclass Members' Personal Data in violation of Nev. Rev. Stat. § 598.0915(15);

d. Defendant engaged in deceptive trade practices with respect to its employment of, and/or business affiliation with, Nevada Subclass Members' and the Personal Data of those Class Members, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the 15 U.S.C. § 45, NRS 603A.210;

e. Defendant engaged in deceptive trade practices by failing to disclose the Data Breach to Nevada Subclass Members in a timely and accurate manner, in violation of NRS 603A.220(1);

f. Defendant engaged in deceptive trade practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Nevada Subclass Members' Personal Data from further unauthorized disclosure, release, data breaches, and theft.

g. Defendant violated NRS 598.0923(3) because its violations of the FTCA, NRS 603A, and NRS 598.0915(15) constituted a violation of a state or federal law.

368. The above unlawful and deceptive acts and practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

369. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Nevada Subclass Members' Personal Information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nevada Subclass.

370. As a direct and proximate result of Defendant's deceptive practices, Nevada Subclass Members suffered injury and/or damages.

371. Under NRS 41.600, violation of either NRS 598.0915 or NRS 598.0923(3) constitutes actionable "consumer fraud."

372. Nevada Subclass Members seek relief under Nev. Rev. Stat. Ann. § 41.600, including, but not limited to, injunctive relief, other equitable relief, actual

damages, and attorneys' fees and costs. These damages, in the aggregate, are in excess of $15,000.

COUNT XV
VIOLATION OF NORTH CAROLINA'S UNFAIR TRADE PRACTICES ACT
(On Behalf of Plaintiff Hill and the North Carolina Subclass)

373. Plaintiff Hill ("Plaintiff," for purposes of this Count) and the North Carolina Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

374. Plaintiff Hill brings this Count on her own behalf and that of the North Carolina Subclass for violations of the North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), et seq.

375. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale, performance, and advertisement of its services, including: (1) failing to maintain adequate data security to keep Plaintiff Hill's and the North Carolina Subclass's sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff Hill and the North Carolina Subclass regarding its lack of adequate data security and inability or unwillingness to properly secure and protect the PII of

Plaintiff Hill and the North Carolina Subclass; (3) failing to disclose or omitting materials facts to Plaintiff Hill and the North Carolina Subclass about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff Hill and the North Carolina Subclass; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Hill and the North Carolina Subclass's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

376. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff Hill and the North Carolina Subclass and defeat their reasonable expectations about the security of their PII.

377. Moreover, Defendant represented that it would maintain the data it collected and custodied in a secure manner and endeavor to keep it safe from unauthorized access and exfiltration.

378. Defendant intended that Plaintiff Hill and the North Carolina Subclass rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

379. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the North Carolina Subclass. Plaintiff Hill and the North Carolina Subclass have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

380. Defendant also violated N.C. Gen. Stat. Ann. § 75-65(a), et seq., by failing to immediately notify Plaintiff Hill and the North Carolina Subclass of the nature and extent of the Data Breach.

381. As a result of Defendant's wrongful conduct, Plaintiff Hill and the North Carolina Subclass were injured in that they never would have provided their PII to Defendant or permitted it to be provided to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

382. As a direct and proximate result of Defendant's violations described herein, Plaintiff Hill and the North Carolina Subclass have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiff Hill and the North Carolina Subclass would not

have made had they known of Defendant's inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

383. Plaintiff Hill and the North Carolina Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of North Carolina's consumer protection statutes.

COUNT XVI
VIOLATION OF OREGON'S UNFAIR TRADE PRACTICES ACT
(On Behalf of Plaintiff Quan and the Oregon Class)

384. Plaintiff Quan ("Plaintiff," for purposes of this Count) and the Oregon Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

385. Plaintiff Quan brings this Count on her own behalf and that of the Oregon Subclass for violations of the Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e)(g) and (u), *et seq*.

386. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale, performance, and advertisement of its services, including: (1) failing to maintain adequate data security to keep Plaintiff Quan's and the Oregon

Subclass's sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff Quan and the Oregon Class regarding its lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff Quan and the Oregon Subclass; (3) failing to disclose or omitting materials facts to Plaintiff Quan and the Oregon Subclass about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff Quan and the Oregon Subclass; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Quan and the Oregon Subclass's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

387. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff Quan and the Oregon Subclass and defeat their reasonable expectations about the security of their PII.

388. Moreover, Defendant represented that it would maintain the data it collected and custodied in a secure manner and endeavor to keep it safe from unauthorized access and exfiltration.

389. Defendant intended that Plaintiff Quan and the Oregon Subclass rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

390. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Oregon Subclass. Plaintiff Quan and the Oregon Subclass have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

391. Defendant also violated Or. Rev. Stat. Ann. § 646A.604(1), et seq. by failing to immediately notify Plaintiff Quan and the Oregon Subclass of the nature and extent of the Data Breach.

392. As a result of Defendant's wrongful conduct, Plaintiff Quan and the Oregon Subclass were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

393. As a direct and proximate result of Defendant's violations described herein, Plaintiff Quan and the Oregon Subclass have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiff Quan and the Oregon Subclass would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

394. Plaintiff Quan and the Oregon Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of Oregon's consumer protection statutes.

COUNT XVII
VIOLATION OF O.C.G.A. § 13-6-11
(On Behalf of Plaintiffs and the Nationwide Class)

395. Plaintiffs and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 178.

396. Defendant through its actions alleged and described herein acted in bad faith, was stubbornly litigious, or caused Plaintiffs and the Class unnecessary trouble and expense with respect to the events underlying this litigation.

397. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to implement and use reasonable measures to protect PII.

398. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII that it obtained and stored and the foreseeable consequences of a data breach.

399. Defendant also has a duty under the Georgia Constitution which contains a Right to Privacy clause, Chapter 1, Article 1, to protect its users' private information. The Georgia Constitution states "no person shall be deprived of life, liberty, or property except by due process of law." Moreover, the Georgia Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

400. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) §652A which specifically recognized four common law invasion of privacy claims in Georgia, which include 1) appropriation

of likeness; 2) intrusion on solitude or seclusion; 3) public disclosure of private facts; and 4) false light.

401. Defendant's implementation of inadequate data security measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required Plaintiffs and the Class to provide and stored on its own servers constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

402. Defendant knew or should have known that it had a responsibility to protect the PII it required Plaintiffs and the Class to provide and stored, that it was entrusted with this PII, and that it was the only entity capable of adequately protecting the PII.

403. Despite that knowledge, Defendant abdicated its duty to protect the PII it required Plaintiffs and the Class provide and that it stored.

404. As a direct and proximate result of Defendant's actions, Plaintiffs' and the Class Members' PII was stolen. As further alleged above, the Data Breach was a direct consequence of Defendant' abrogation of data security responsibility and its decision to employ knowingly deficient data security measures that knowingly left the PII unsecured. Had Defendant adopted reasonable data security measures, it could have prevented the Data Breach.

405. As further described above, Plaintiffs and the Class have been injured and suffered losses directly attributable to the Data Breach.

406. Plaintiffs and the Class therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against Defendant and that the Court grant the following:

a. For an Order certifying the Class and Subclasses as defined herein, and appointing Plaintiffs and their counsel to represent the Class and Subclasses;

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 the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and the 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 its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;

iv. requiring Defendant to delete, destroy, and purge the personally 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;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the

confidentiality and integrity of the personally identifying information of Plaintiffs and Class Members;

vi. prohibiting Defendant from maintaining Plaintiffs and Class Members' personally identifying information on a cloud-based database;

vii. 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;

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

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

x. 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 areas of Defendant's systems;

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

xii. 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 personally identifying information, as well as protecting the personally identifying information of Plaintiffs and Class Members;

xiii. 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;

xiv. 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 personally identifying information;

xv. 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;

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

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and, for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to Class Counsel, and to report any material deficiencies or noncompliance with the Court's final judgment;

d. That the Court award Plaintiffs, the Class and Subclass members damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

e. That the Court order disgorgement and restitution of all earnings, profits, compensation and benefits received by Defendant as a result of its unlawful acts, omissions and practices;

f. For expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11 and as otherwise allowed by law;

g. For prejudgment and post-judgment interest on all amounts awarded; and,

h. Such other and further relief as this Court may deem just and proper.

VII. JURY TRIAL DEMAND

Plaintiffs hereby demand that this matter be tried before a jury.

DATED: July 13, 2022.

Respectfully submitted,

THE FINLEY FIRM, P.C.
/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
N. Nickolas Jackson
Georgia Bar No. 841433
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Telephone: (404) 320-9979
Fax: (404) 320-9978

Interim Liaison Counsel for Plaintiffs

Kenya J. Ready
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Phone: (813) 202-7185
Fax: (813) 222-4738

Gary M. Klinger**
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
Email: gklinger@milberg.com

Terence R. Coates**
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
Email: tcoates@msdlegal.com

Interim Co-Lead Counsel for Plaintiffs

M. Anderson Berry**
Gregory Haroutunian**
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

David K. Lietz*
MILBERG COLEMAN BRYSON

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

Joseph M. Lyon**
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Telephone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Gregory J. Bosseler
MORGAN & MORGAN
191 Peachtree St. NE. Ste. 4200
Atlanta, GA 30303
Telephone: (404) 496-7318
gbosseler@forthepeople.com

John A. Yanchunis**
Patrick Barthle**
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
jyanchunis@forthepeople.com
pbrathle@forthepeople.com

Bryan L. Bleichner**
CHESTNUT CAMBRONNE PA
100 Washington Ave. South, Ste. 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

Jonathan M. Lebe*
Nicolas W. Tomas*
LEBE LAW, APLC
777 S. Alameda Street, Second Floor
Los Angeles, CA 90021

Counsel for Plaintiffs

**pro hac vice forthcoming*
***pro hac vice*

CERTIFICATE OF SERVICE & COMPLIANCE

I hereby certify that on this date I served the foregoing **Consolidated Class Action Complaint** via the CM/ECF system, which will automatically provide-email notification and service of such filing to counsel of record for all parties registered with the Court for electronic filing.

I further certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

This 13th day of July, 2022.

/s/ MaryBeth V. Gibson
MARYBETH V. GIBSON