Nathan R. Ring
NV Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Blvd., Ste. 208
Las Vegas, NV 89102
(725) 235-9750
nring@stranchlaw.com

Miles Schiller (application for admission pro hac vice forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Ave., Suite 200
Nashville, Tennessee 37203
(615) 254-8801
mschiller@stranchlaw.com

Jeff Ostrow (application for admission pro hac vice forthcoming)
Ken Grunfeld (application for admission pro hac vice forthcoming)
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
E: ostrow@kolawyers.com
grunfeld@kolawyers.com

Counsel for Plaintiff and the Putative Class

FIRST JUDICIAL DISTRICT COURT

IN AND FOR CARSON CITY, STATE OF NEVADA

BERT TIPTON, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

CASINO FANDANGO L.L.C., a Nevada limited liability company,

Defendant.

Case No. 24OC00018-1B

Dept No. I

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Bert Tipton, individually and on behalf of all similarly situated persons, alleges the following against Casino Fandango LLC ("Defendant") based on personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents, as to all other matters.

I. NATURE OF THE ACTION

1. This class action arises out of the cyberattack and data breach of which Defendant became aware of in June 2024 ("Data Breach") resulting from Defendant's failure to implement reasonable and industry standard data security practices.

2. Defendant is a hotel casino resort offering a variety of slot machines, table games, sports book, restaurants, and bars.[1]

3. Plaintiff's and Class Members' sensitive personal information – including name, and Social Security number ("PII"), which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

4. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who targeted the Private Information for its value to identity thieves.

5. As a result of the Data Breach, Plaintiff and Class Members, suffered concrete injuries in fact including, but not limited to: (i) Plaintiff's Private Information being disseminated on the dark web; (ii) Plaintiff experiencing an increase in spam calls, texts, and/or emails; (iii) lost or diminished value of their Private Information; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (v) invasion of privacy; (vi) loss of benefit of the bargain; and (vii) the continued and

1 *See* https://casinofandango.com/ (last visited Oct. 24, 2024).

certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its patients' Private Information from a foreseeable and preventable cyber-attack.

7. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

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

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

10. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, e.g., opening new financial accounts or making transactions in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain

government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft, as well as embarrassment, loss of employment opportunities and invasion of privacy. Plaintiff and Class Members must now and in the future closely monitor their accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs, e.g., for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

14. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

II. PARTIES

16. Plaintiff Bert Tipton is a natural person and citizen of Nevada.

17. Defendant is a Nevada limited liability company with its principal place of business located in Carson City, Nevada.

III. JURISDICTION AND VENUE

18. Jurisdiction is proper in this Court pursuant to NRS 14.065. Jurisdiction is proper in

this Court because a substantial part of the actions and omissions taken by Defendant occurred within Carson City, Nevada and the amount in controversy is greater than $15,000.

19. Venue is proper in this Court pursuant to NRS 13.010. Venue is proper in this Court because Defendant resides in Carson City, Nevada; Defendant conducts business and directed its actions in Carson City, Nevada; and a substantial part of the actions giving rise to these claims occurred in Carson City, Nevada.

IV. BACKGROUND FACTS

A. Defendant's Business

20. "Casino Fandango is a casino resort in Carson City, Nevada. Casino Fandango offers table games, slots, keno, and a sports book. The resort also has a 100-room "Courtyard by Marriott" hotel and five restaurants. Casino Fandango employs more than 311 people."[2]

21. Defendant obtains from its employees their PII as part of the employee-employer relationship, and as a condition of providing employment.

22. On or about June 8, 2024, Plaintiff's and Class Members' PII in Defendant's possession was obtained by an unauthorized party, which Defendant describes in its Notice Letter as "a cybersecurity event" which resulted in certain files being accessed and/or acquired by an unauthorized actor."[3]

23. Approximately three months later, on September 23, 2024, Defendant filed a notice of data breach with Attorney General of Montana, indicating that the cybersecurity incident was a cyberattack. Three months after the Data Breach, Defendant began sending out Notice Letters to affected persons, informing them that their PII had been compromised in the Data Breach.[4]

---

[2] *See* https://www.jdsupra.com/legalnews/casino-fandango-files-official-notice-2679576/ (last visited Oct. 24, 2024).

[3] Ex. A.

[4] *See id.*

24. The Notice Letter states Defendant "launched an investigation into the nature and scope of the event. Through our investigation, we determined that certain computer systems were accessed by an unauthorized actor and some information was copied from these systems between June 8, 2024 and June 13, 2024. We conducted a comprehensive review of the involved files to determine what information was present in these files and to whom the information related."[5]

25. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as a hotel and casino resort that collects, creates, and maintains PII on its computer networks and/or systems.

26. As evidenced by the Data Breach, the PII contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

B. Defendant Fails to Safeguard Consumer PII.

27. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay." [6]

28. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to

---

[5] *Id*

[6] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNET, (April 30, 2020 2:43ntiffPM) https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/.

release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[7]

29. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement have difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

30. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[8]

31. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[9]

32. 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, PII can be sold at a price ranging from $40 to $200, and bank details have

---

[7] *See* https://www.cisa.gov/sites/default/files/2023-01-CISA_MSISAC_Ransomware%20Guide_8508C.pdf.

[8] *Shining a Light on the Dark Web with Identity Monitoring,* IDENTITYFORCE, (Dec. 28, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring.

[9] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR, (April 3, 2018), https://www.armor.com/resources/blog/stolen-pii- ramifications- identity-theft-fraud-dark-web.

a price range of $50 to $2009.[10] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[11] Criminals can also purchase access to entire company data breaches.[12]

33. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

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

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

36. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

37. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts,

---

[10] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal- data-sold-on-the-dark-web- how-much-it-costs/.

[11] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is- selling-for-on-the-dark-web/ (last visited Oct. 24, 2024).

[12] *In the Dark*, VPN Overview, 2019, https://vpnoverview.com/privacy/anonymous- browsing/in-the- dark/ (last visited Oct. 24, 2024).

receive government benefits, and make purchases and secure credit in a victim's name.[13] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[14]

38. The market for PII has continued unabated to the present, and in 2023 the number of reported data breaches in the United States increased by 78% over 2022, reaching 3205 data breaches.[15]

39. The exposure of Plaintiff's and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

C. Defendant was on Notice of the Foreseeable Risk of the Data Breach.

40. In light of recent high profile data breaches, Defendant knew or should have known the electronic records and PII it maintained would be targeted by cybercriminals and ransomware attack groups.

41. Hospitality industry entities are prime targets for cyberattacks because of the information they collect and store, including financial information, names, social security

---

[13] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf (last visited Oct. 24, 2024).

[14] *Id.*

[15] Beth Maundrill, *Data Privacy Week: US Data Breaches Surge, 2023 Sees 78% Increase in Compromises*, INFOSECURITY MAGAZINE (Jan. 23, 2024); https://www.infosecurity-magazine.com/news/us-data-breaches-surge-2023/ (last visited Oct. 24, 2024); *see also* Identity Theft Resource Center, *2023 Data Breach Report*, https://www.idtheftcenter.org/publication/ 2023-data-breach-report/ (last visited Oct. 24, 2024).

numbers, and driver's license numbers—all extremely valuable in underground markets.

42. This was known and obvious to Defendant, as it observed frequent public announcements of data breaches affecting the hospitality industry and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of cybercriminals.

43. For example, Marriot International, Inc.'s "failure to implement reasonable data security led three large data breaches from 2024 to 2020 impacting more that 344 million customers worldwide.[16]

44. Additionally, cyber security experts have explained that "hotels are an attractive target for hackers because they hold a lot of sensitive information, including credit card and passport details, but often don't have security standards as tough as those of more regulated industries, like banking."[17]

45. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[18] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[19]

46. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to companies storing sensitive PII, like Defendant.

---

[16] *FTC Takes Action Against Marriott and Starwood Over Multiple Data Breaches*, FTC.GOV (Oct. 9, 2024), http://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches

[17] *Breach Puts Hotel Guests' Data at Risk*, ARKANSAS DEMOCRAT (Dec. 1, 2018), http://www.arkansasonline.com/news/2018/dec/01/breach-puts-hotel-guests-data-at-risk-2/.

[18] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

[19] *Id.*

47. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and the foreseeable consequences that would occur if its data security systems were breached, including, specifically, the significant costs that would be imposed on affected individuals as a result of the breach.

48. Defendant was, or should have been, fully aware of the significant number of individuals whose PII it collected and stored, thus, the significant number of individuals who would be harmed by a breach of Defendant's systems.

49. Despite all the publicly available knowledge of the serious threat of compromises of personal information and despite holding the PII of thousands of individuals, Defendant failed to use reasonable care in maintaining the privacy and security of Plaintiff's and Class Members' PII. Had Defendant implemented adequate security measures, cybercriminals never could have accessed potentially thousands of individuals' files and the Data Breach would have been prevented or much smaller in scope.

D. Defendant Fails to Comply with FTC Guidelines.

50. 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.

51. 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 customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security

problems.[20] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[21]

52. 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.

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

54. These FTC enforcement actions include actions against private universities like Defendant.

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

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

57. Defendant was at all times fully aware of its obligation to protect the PII. Defendant

---

[20] *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.

[21] *Id.*

was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Fails to Comply with Industry Standards.

58. Several best practices have been identified that at a minimum should be implemented by companies storing sensitive PII 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.

59. Other best cybersecurity practices that are standard 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; training staff regarding critical points.

60. 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.

61. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

F. Defendant's Breach

62. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and website's application flow. 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 and cyber-attacks;

b. failing to adequately protect PII;

c. failing to properly monitor their own data security systems for existing intrusions;

d. failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

f. failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

g. failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

i. failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII;

j. failing to train all members of their workforces effectively on the policies and procedures regarding PII;

k. failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

l. failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTCA;

m. failing to adhere to industry standards for cybersecurity as discussed above; and,

n. otherwise breaching their duties and obligations to protect Plaintiff's and

Class Members' PII.

63. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access Defendant's computer systems, which provided unauthorized actors with unsecured and unencrypted PII.

64. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

G. Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft.

65. Cyberattacks and data breaches at businesses like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

66. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[22]

67. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such

---

[22] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, U.S. GOV. ACCOUNTING OFFICE, (2007) https://www.gao.gov/new.items/d07737.pdf.

as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

68. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[23]

69. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

70. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

71. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[24]

---

[23] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps.

[24] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

72. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

73. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

74. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

75. 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.

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

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

78. PII can sell for as much as $363 per record according to the Infosec Institute.[26] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once

---

[25] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, U.S. GOV. ACCOUNTING OFFICE, (2007) https://www.gao.gov/new.items/d07737.pdf.

[26] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

PII is stolen, fraudulent use of that information and damage to victims may continue for many years.

79. 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.[27] 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.[28] Each of these fraudulent activities is difficult to detect. An individual may not know that their 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.

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

81. 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."[29]

82. 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

---

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

[28] *Id* at 4.

[29] 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.

than 10x on the black market."[30]

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

H. Plaintiff's and Class Members' Damages

84. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

85. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

86. Upon information and belief, Plaintiff and Class Members' PII, including names and Social Security numbers, were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's software maintaining PII. This PII was acquired by some unauthorized, unidentified third-party threat actor.

87. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

88. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis trying to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring their accounts for fraudulent activity.

89. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

90. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members

---

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

have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

91. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

92. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

93. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

94. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

95. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

96. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and sensitive information for misuse.

97. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. purchasing credit monitoring and identity theft prevention;

c. placing "freezes" and "alerts" with reporting agencies;

d. spending time on the phone with or at financial institutions and government

agencies to dispute unauthorized and fraudulent activity in their name;

e. contacting financial institutions and closing or modifying financial accounts; and

f. closely reviewing and monitoring Social Security numbers, bank accounts, and credit reports for unauthorized activity for years to come.

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

99. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

100. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

I. Plaintiff's Experience

Plaintiff Bert Tipton

101. Plaintiff Bert Tipton provided his information to Defendant as a condition of employment.

102. Plaintiff was employed with Defendant from 2021 to July 2024.

103. Plaintiff provided his PII to Defendant and trusted that it would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

104. Upon information and belief, Plaintiff's PII was compromised in the Data Breach.

105. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

106. Defendant has deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it in a timely manner.

107. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after learning of the Data Breach.

108. Plaintiff has spent significant time attempting to mitigate the impact of the Data Breach and will continue to spend valuable hours for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

109. As a result of the Data Breach, Plaintiff has suffered stress due to his information being exposed and impacting his credit.

110. Plaintiff 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 maintained belonging to Plaintiff; (b) violation of his privacy rights; (c) the theft of his PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

111. As a result of the Data Breach, Plaintiff has also suffered emotional distress 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 is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

112. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

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

CLASS ACTION ALLEGATIONS

114. Plaintiff brings this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") pursuant to Nevada Rule of Civil Procedure 23.

115. Plaintiff propose the following Class subject to amendment as appropriate:

All persons whose PII was compromised in the Data Breach ("Class").

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

117. Plaintiff reserves the right to amend or modify the Class definitions as this case progresses.

118. The proposed Class meets the criteria for certification under Nevada Rules of Civil Procedure 23(a) & (c).

119. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

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

a. if Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. if 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. if Defendant's data security systems prior to and during the Data Breach

complied with applicable data security laws and regulations;

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

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

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

g. if Defendant knew or should have known that their data security systems and monitoring processes were deficient;

h. if Defendant should have discovered the Data Breach sooner;

i. if Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. if Defendant's conduct was negligent;

k. if Defendant's breach implied contracts with Plaintiff and Class Members;

l. if Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. if Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. if Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

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

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

123. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from

Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

124. 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.

125. Class certification is also appropriate under Nevada Rule of Civil Procedure 23(c)(2). Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

126. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

127. Plaintiff repeat and re-allege paragraphs 1 through 126 above as if fully set forth herein.

128. Defendant require their employees to submit non-public PII as a condition of services.

129. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its

business, which affects commerce.

130. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that the information would be safeguarded.

131. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if their PII were wrongfully disclosed.

132. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

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

134. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand. That special relationship arose because Defendant was entrusted with their confidential PII, a necessary part of employment with Defendant.

135. Defendant also had a duty to exercise appropriate clearinghouse practices to remove current and former employees' PII they were no longer required to retain pursuant to regulations.

136. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach, but failed to do so.

137. Defendant had and continues to have duties to adequately disclose that Plaintiff's and Class Members' PII within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

138. Defendant breached its duties and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. The specific negligent acts and omissions

committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former employees' PII they were no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

139. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

140. Defendant knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' PII would cause damage to Plaintiff and the Class.

141. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

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

143. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was

reasonably foreseeable given the known high frequency of corporate cyberattacks and data breaches.

144. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

145. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting, storing and maintaining PII, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on its systems.

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

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

148. Defendant's duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

149. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

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

151. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' PII, and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care by adopting, implementing, and maintaining appropriate security measures.

152. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by Defendant's data breach; (x) the value of the unauthorized access to their PII permitted by Defendant; and (xi) any nominal damages that may be awarded.

153. As a direct and proximate result of Defendant's negligence, Plaintiff 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 including nominal damages.

154. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

155. Defendant's negligent conduct is ongoing, in that it still possesses Plaintiff's and Class Members' PII in an unsafe and insecure manner.

156. Plaintiff and Class Members are entitled to injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

157. Plaintiff repeat and re-allege paragraphs 1 through 126 above as if fully set forth herein.

158. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of employment.

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

160. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

161. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

162. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing. The mutual understanding is also evidenced by statements in Defendant's privacy policy, https://casinofandango.com/privacy-policy/.

163. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their

Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

164. In accepting the Private Information of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

165. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

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

167. Plaintiff and Class Members paid money and provided their Private Information to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

168. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

169. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

170. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

171. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

172. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members were injured, as alleged herein, including the loss of the benefit of the bargain.

173. Plaintiff and Class Members are entitled to compensatory, consequential, and/or nominal damages suffered as a result of the Data Breach.

174. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

175. Plaintiff repeat and re-allege paragraphs 1 through 126 above as if fully set forth herein.

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

177. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

178. The unauthorized disclosure and/or acquisition (*i.e.,* theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

179. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

180. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

181. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

182. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

183. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

184. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

185. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

186. Plaintiff, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

187. Plaintiff, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

188. Plaintiff repeat and re-allege paragraphs 1 through 126 above as if fully set forth herein.

189. This count is pleaded in the alternative to breach of implied contract.

190. Plaintiff and Class Members conferred a monetary benefit on Defendant in connection with employment, specifically providing Defendant, with their PII.

191. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and use Plaintiff's and Class Members' PII for business purposes.

192. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

193. Defendant acquired the PII through inequitable record retention as it failed to disclose the inadequate vendor vetting and data security practices previously alleged.

194. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

195. As a direct an proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by Defendant's data breach; (x) the value of the unauthorized access to their PII permitted by Defendant; and (xi) any nominal damages that may be awarded.

196. Plaintiff and Class Members are entitled to restitution and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct, as well as return of their sensitive PII and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

197. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

FIFTH CAUSE OF ACTION
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiff and the Class)

198. Plaintiff repeat and re-allege paragraphs 1 through 126 above as if fully set forth herein.

199. 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 to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

200. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff allegeS Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

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

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals

of the Data Breach under the common law and Section 5 of the FTCA;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

202. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its prospective, current and/or former employees (i.e., Plaintiff's and the Class's) data.

203. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

204. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

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

PRAYER FOR RELIEF

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

A. For an Order certifying the Class, and appointing Plaintiff and their Counsel to

represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

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

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

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

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

iv. requiring Defendant to 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 Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members 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 portions 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 personal identifying information, as well as protecting the personal identifying information of Plaintiff 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

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

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 counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, consequential, and punitive damages, as allowed by law in an amount to be determined, believed to be well in excess of $15,000;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

AFFIRMATION

The undersigned affirms that this pleading does not contain personal information as defined in NRS 239B.030(4), and acknowledge that when they file any additional documents, an affirmation will be provided only if the document does contain personal information.

Dated: October 29, 2024

Respectfully submitted,

Nathan R. Ring
NV Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Blvd., Ste. 208
Las Vegas, NV 89102
(725) 235-9750
nring@stranchlaw.com

Miles Schiller (application for admission *pro hac vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Ave., Suite 200
Nashville, Tennessee 37203
(615) 254-8801
mschiller@stranchlaw.com

Jeff Ostrow (application for admission *pro hac vice* forthcoming)
Ken Grunfeld (application for admission *pro hac vice* forthcoming)
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
E: ostrow@kolawyers.com
grunfeld@kolawyers.com

Counsel for Plaintiff and the Putative Class