Don Springmeyer, Esq. (SBN 1021)
Daniel Bravo, Esq. (SBN 13078)
A. Jill Guingcangco, Esq. (SBN 14717)
WOLF, RIFKIN, SHAPIRO, SCHULMAN & RABKIN, LLP
3556 E. Russell Road, 2nd Floor
Las Vegas, Nevada 89120
Telephone: (702) 341-5200 / Fax: (702) 341-5300
Email: dspringmeyer@wrslawyers.com
Email: dbravo@wrslawyers.com
Email: ajg@wrslawyers.com

BURSOR & FISHER, P.A.
Yitzchak Kopel (*Pro Hac Vice Forthcoming*)
Max S. Roberts (*Pro Hac Vice*)
888 Seventh Avenue, Third Floor
New York, NY 10019
Telephone: (646) 837-7150 / Fax: (212) 989-9163
Email: ykopel@bursor.com
Email: mroberts@bursor.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

JENNIFER MIRANDA and PATRICIA TERRY, on behalf of themselves and all others similarly situated, Plaintiffs, v. GOLDEN ENTERTAINMENT (NV), INC., Defendant.	Case No.: 2:20-cv-00534-JAD-DJA **FIRST AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND**

Jennifer Miranda and Patricia Terry (collectively, "Plaintiffs") bring this action on behalf of themselves and all others similarly situated against Defendant Golden Entertainment (NV), Inc. ("Golden Entertainment" or "Defendant"). Plaintiffs make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to the allegations specifically pertaining to themselves, which are based on personal knowledge.

/ / /

/ / /

/ / /

NATURE OF THE ACTION

1. Golden Entertainment is a large gaming corporation that owns numerous casinos in Nevada and Maryland. Among these properties are Arizona Charlie's Hotel & Casino in Las Vegas, the Pahrump Golden Nugget Hotel & Casino in Pahrump, Nevada, PT's Gold Pub in Las Vegas, and the Strat Hotel & Casino in Las Vegas, which is the tallest structure in Nevada and one of Las Vegas' most iconic casinos.

2. Between May 30, 2019 and October 6, 2019, Golden Entertainment was the subject of a data breach due to its negligent failure to properly safeguard the information of its customers and employees. The data breach exposed the "names, Social Security numbers, passport numbers, government ID numbers, driver's license numbers, dates of birth, usernames, passwords, payment card numbers, expiration dates, card security codes (CVV), financial account numbers, routing numbers, health insurance information, and health or treatment information" (collectively, the "personal identification information" or "PII") of Golden Entertainment's customers, current and former employees, and vendors.[1]

3. Plaintiffs bring this class action on behalf of themselves and all others similarly situated for actual and statutory damages, as well as punitive damages and equitable relief to fully redress the widespread harm Golden Entertainment's wrongful acts and omissions have unleashed.

THE PARTIES

4. Plaintiff Jennifer Miranda is a citizen of Nevada who resides in Clark County, Nevada. Ms. Miranda worked at PT's Gold Pub, one of Defendant's properties, between 2015 and 2016. As part of her employment, Ms. Miranda entrusted her PII, including her Social Security Number, to Defendant. When entrusting her PII to Defendant, Ms. Miranda reasonably believed that her PII would be securely stored and protected against unauthorized access. In fact, Defendant represented in its Privacy Policy that it uses "reasonable organizational, technical, and

[1] NOTICE OF DATA SECURITY INCIDENT, https://www.goldenent.com/emailsecurityincident/index.html (last accessed Feb. 25, 2020).

administrative measures designed to protect Personal Information within our organization." Defendant never disclosed to Ms. Miranda that her PII would be stored long after she stopped working at their establishment. In or about December 2019, Ms. Miranda received a letter from Defendant informing her that her PII—including her name and Social Security number—was accessed and extracted in the data breach. Ms. Miranda now faces a substantial and imminent risk of fraud, identity theft, and long-term adverse effects as a result of her PII being compromised. In fact, Ms. Miranda was already the victim of identity theft in October 2019 when an unauthorized user gained access to Ms. Miranda's banking account. This unauthorized user opened up a fraudulent username on Ms. Miranda's bank account, which Ms. Miranda had to have removed. As part of dealing with the identity theft, Ms. Miranda paid for Experian's credit reporting service, which costs her $9.99 a month. Ms. Miranda made these payments prior to receiving any notice of the data breach from Defendant. Further, Ms. Miranda was forced to lock her credit report so that the unauthorized user could not affect her credit score. Ms. Miranda had to unlock her credit report each time she wanted to access it. As Ms. Miranda was looking for a house at the time that the identity theft occurred, this was a particularly inconvenient process for Ms. Miranda. Ms. Miranda spent two weeks of sustained agony dealing with the identity theft, and Ms. Miranda now uses additional credit reporting services—Credit Karma and Credit Sesame—to protect herself from further harm. Upon information and belief, this identity theft was the result of the Golden Entertainment data breach.

5. Plaintiff Patricia Terry is a citizen of Nevada who resides in Clark County, Nevada. Ms. Terry is a regular customer and guest at Arizona Charlie's Hotel & Casino, one of Defendant's properties, for 15 years, and last visited Arizona Charlie's in February 2020. As part of staying and using the facilities at Arizona Charlie's, Ms. Terry entrusted her PII, including her Social Security Number, to Defendant. When entrusting her PII to Defendant, Ms. Terry reasonably believed that her PII would be securely stored and protected against unauthorized access. In fact, Defendant represented in its Privacy Policy that it uses "reasonable organizational, technical, and administrative measures designed to protect Personal Information within our organization." In or about February 2020, Ms. Terry received a letter from Defendant

informing her that her PII—including her name, Social Security number, and driver's license number—was accessed and extracted in the data breach. Ms. Terry now faces a substantial and imminent risk of fraud, identity theft, and long-term adverse effects as a result of his PII being compromised. In fact, Ms. Terry was already the victim of identity theft in February 2020 when an unauthorized user opened up a DirecTV account in Ms. Terry's name. Ms. Terry discovered this in June 2020 when she checked her credit score and noticed a "derogatory mark" on her credit score filed by Enhanced Recovery Company. The derogatory mark was for an outstanding DirecTV bill of $981.00 that was opened in February 2020. Ms. Terry does not owe any debt to DirecTV. Ms. Terry had to spend several hours on the phone calling DirecTV and Enhanced Recovery Company in order to have the debt declared as fraud. Meanwhile, this "debt" has negatively impacted Ms. Terry's credit score by over 20 points.

6. Defendant Golden Entertainment (NV), Inc. is a Minnesota corporation with a principal place of business at 6595 S Jones Boulevard, Las Vegas, NV 89118. Golden Entertainment does substantial business in the State of Nevada, and its casinos and hotels attract customers from across the United States.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 members of the Class, the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from Defendant. This Court has supplemental jurisdiction over state law claims pursuant to 28 U.S.C. § 1367.

8. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in Las Vegas, Nevada.

9. Venue is proper in this District pursuant to 28 U.S.C. § 1391 as Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

I. BACKGROUND ON DATA BREACHES

10. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.[2]

11. A data breach can occur in numerous ways. One way that a data breach can occur, and most relevant to this action, is through phishing. Phishing occurs when a hacker "mimics a trusted, reputable entity in order to collect sensitive data," particularly banking information or highly personal details.[3] Phishing is done through pop-ups on internet browsers, emails with a link, or even phone calls where the hacker pretends to work for a reputable company.[4]

12. Data breaches are becoming increasingly more common and harmful. In 2014, 783 data breaches were reported, with at least 85.61 million total records exposed.[5] In 2019, 3,800 data breaches were reported, with at least 4.1 billion total records exposed.[6] The average cost of a data breach in the United States in 2019 was $8.19 million.[7]

13. Consumers are harmed in a variety of ways by data breaches. First, consumers are harmed financially. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150.00 per record.[8]

---

[2] Julian De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN (Oct. 24, 2019), https://digitalguardian.com/blog/history-data-breaches (last accessed Feb. 25, 2020).

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] Dan Rafter, *2019 Data Breaches: 4 Billion Records Breached So Far*, NORTON BY SYMANTEC, https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html (last accessed Feb. 25, 2020).

[7] Chris Brook, *What's the Cost of a Data Breach in 2019*, DIGITAL GUARDIAN (July 30, 2019), *https*://digitalguardian.com/blog/whats-cost-data-breach-2019 (last accessed Feb. 25, 2020).

[8] *Id.*

However, other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft—a common result of data breaches—was $298.00 dollars.[9] And in 2019, Javelin Strategy & Research compiled consumer complaints from the U.S. Federal Trade Commission ("FTC") and indicated that the median out-of-pocket cost to consumers for identity theft was $375.00.[10]

14. Identity theft is one of the most problematic harms resulting from a data breach. With access to an individual's PII, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture. In addition, identity thieves may obtain a job, rent a house, or receive medical services in the victim's name. Identity thieves 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.[11]

15. Consumers are also harmed by the time they spend rectifying the effects of a data breach. A Presidential identity theft report from 2007 states that:

> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts, open new ones, and dispute charges with individual creditors.[12]

---

[9] NORTON BY SYMANTEC, 2013 NORTON REPORT 8 (2013), https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf (last accessed Feb. 25, 2020).

[10] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last accessed Feb. 25, 2020) (citing the Javelin report).

[11] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Feb. 24, 2020).

[12] U.S. FEDERAL TRADE COMMISSION, THE PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 11 (2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-

16. Further, the effects of a data breach on consumers are not temporary. In a report issued by the U.S. Government Accountability Office ("GAO"), the GAO found that "stolen data may be held for up to a year or more before being used to commit identity theft," and "fraudulent use of [stolen information] may continue for years" after the stolen information is posted on the Internet.[13] This is particularly the case in data breaches involving Social Security numbers, where the risk of identity fraud remains elevated for several years to throughout a person's entire life."[14] In fact, consumers suffer 33% of the harm from a data breach after the first year.[15] Thus, consumers can lose years' worth of time dealing with a data breach.

II. THE GOLDEN ENTERTAINMENT DATA BREACH

17. Between May 30, 2019 and October 6, 2019, Golden Entertainment was the subject of a data breach. The data breach was conducted through an email phishing incident by an unauthorized user. Through this email phishing incident, the unauthorized user obtained access to some employees' email accounts.

18. On October 8, 2019, and again on January 3, 2020, Golden Entertainment conducted an investigation into the email phishing incident and determined that "an email or an attachment to an email in the email accounts contained names, Social Security numbers, passport numbers, government ID numbers, driver's license numbers, dates of birth, usernames, passwords, payment card numbers, expiration dates, card security codes (CVV), financial account numbers, routing numbers, health insurance information, and health or treatment

---

plan/strategicplan.pdf (last accessed Feb. 25, 2020).

[13] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (7th Cir. 2015) (citing U.S. GOV'T ACCOUNTABILITY OFFICE, GAO–07–737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION (2007)).

[14] Alicia Grzadkowska, *Consumers' Data Exposed for Years Following Breach Incidents*, INSURANCE BUSINESS MAG. Sept. 19, 2019, https://www.insurancebusinessmag.com/us/news/cyber/consumers-data-exposed-for-years-following-breach-incidents-178390.aspx (last accessed Feb. 25, 2020).

[15] Larry Ponemon, *What's New in the 2019 Cost of a Data Breach Report*, SECURITY INTELLIGENCE, https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/ (last accessed Feb. 25, 2020).

information" of Golden Entertainment's customers, current and former employees, and vendors."[16]

19. Golden Entertainment began mailing out letters to affected individuals between November 7, 2019 and January 31, 2020. Upon information and belief, as of the date of this Complaint, not all individuals have received their notice letter of the data breach.

20. The data breach affected individuals across the United States.

21. None of the individuals whose PII was accessed, authorized such access or extraction.

22. Golden Entertainment represents in its Privacy Policy that it uses "reasonable organizational, technical, and administrative measures designed to protect Personal Information within our organization."[17] Despite this representation, Golden Entertainment failed to take reasonable measures to protect the PII of Plaintiffs and members of the Class, included the following:

(a) Failing to maintain appropriate technological and other systems to prevent unauthorized access. Despite Golden Entertainment's claim that it uses "reasonable … technical … measures" to protect sensitive data, Golden Entertainment's system was still subject to a data breach.

(b) Failing to properly train its employees to avoid email phishing scams and other potential causes of data breaches. Despite Golden Entertainment's claim that it uses "reasonable organizational … and administrative measures" to protect sensitive data, Golden Entertainment's employees were unable to recognize a phishing scam, one of the most common methods of a data breach.

(c) Failing to minimize the PII that any intrusion could compromise (i.e., less aggregation and weeding out unnecessary and stale data). The data breach

---

[16] NOTICE OF DATA SECURITY INCIDENT, *supra* note 1.

[17] GOLDEN ENTERTAINMENT PRIVACY POLICY, https://goldenent.com/privacy/ (last accessed June 24, 2020).

affected not only current customers and employees of Golden Entertainment, but former employees and customers as well. For instance, Plaintiff Miranda had not worked for Golden Entertainment in nearly five years, yet Golden Entertainment was still holding her PII on its servers.

(d) Failing to provide timely notice to affected consumers with accurate information so that those affected could begin minimizing the impact of the incident. The data breach occurred in May 2019, yet Golden Entertainment did not begin notifying consumers until November 2019. Some consumers, including Plaintiff Miranda, did not receive notice of the data breach until they had already suffered identify theft, by which time Golden Entertainment's notice was meaningless.

23. Although Golden Entertainment is offering individuals whose Social Security numbers or driver's license was accessed through the data breach complimentary credit monitoring and identity protection services through Experian, these "remedies" are inadequate and are too little too late. First, as noted above, Plaintiff Miranda was already the victim of identity theft before she received the letter and the offer for credit monitoring and identity protection services from Defendant. As such, Plaintiff Miranda and others like her were harmed before Golden Entertainment took any remedial action. Second, much of the harm from a data breach can happen years after the data breach occurs. In fact, identity thieves may simply calendar the date that the credit monitoring services are set to expire and act then, as "they don't mind hanging on until they get over that time period."[18] And third, many credit reporting services, including Experian, offer free versions of their services. To wit, Golden Entertainment's offer for complimentary membership is hollow. Thus, the remedial action by Golden Entertainment is inadequate to rectify the harm caused to Plaintiffs and others similarly situated by the data breach.

24. Plaintiffs bring this action on behalf of themselves, the Class, and the Subclass for actual and statutory damages, as well as punitive damages for: (i) negligence; (ii) negligent

[18] Grzadkowska, *supra* note 14.

misrepresentation; (iii) negligence per se for violation of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45; (iv) negligence per se for violation of the Nevada Data Breach Law ("NDBL"), NRS §§ 603A.010, *et seq.*; (v) breach of contract; and (vi) violation of the Nevada Deceptive Trade Practices Act ("NDTPA"), NRS §§ 598.0903, *et seq*.

CLASS ACTION ALLEGATIONS

25. Plaintiffs seek to represent a class defined as all persons or business entities in the United States whose PII was maintained on the servers of Golden Entertainment that were compromised as a result of the data breach (the "Class"). Excluded from the Class are Defendant, its affiliates, employees other than those affected by the data breach, officers and directors, and the Judge(s) assigned to this case.

26. Subject to additional information obtained through further investigation and discovery, the above-described Class may be modified or narrowed as appropriate, including through the use of multi-state subclasses.

27. At this time, Plaintiffs do not know the exact number of members of the Class. However, given the nature of the claims and the size of Defendant's business, Plaintiffs believe that the members of the Class are so numerous that joinder of all members is impracticable.

28. Common questions of law and fact exist as to all members of the Class. The data breach was generally applicable to all members of the Class and arose from a common set of acts and omissions by Defendant without regard to the nature or identity of individual members of the Class, thereby making appropriate relief with respect to the Class as a whole.

29. The questions of law and fact common to the Class include:

(a) Whether Defendant owed a duty to the members of the Class under federal or state law to protect the PII, provide timely notice of the unauthorized access, provide timely and accurate information as to the extent of the compromised PII, and provide meaningful and fair redress;

(b) Whether Defendant breached such a duty;

(c) Whether Defendant's breach provided the means for the data breach;

(d) Whether Defendant was negligent in failing to design, employ, and maintain adequate security systems and protocols;

(e) Whether Defendant's negligence provided the means for the data breach;

(f) Whether Defendant knew or reasonably should have known of the vulnerabilities in its systems that allowed for the unauthorized access;

(g) Whether Defendant falsely represented that it uses "reasonable organizational, technical, and administrative measures designed to protect Personal Information within our organization";

(h) Whether Defendant properly trained its employees, officers, and other members of its staff to avoid potential causes of data breaches;

(i) The appropriate injunctive and related equitable relief for the Class; and

(j) The appropriate class-wide measure of damages for the Class.

30. Plaintiffs' claims are typical of the claims of the members of the Class, and Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs and all members of the Class are similarly affected by Defendant's wrongful conduct in that their PII has been exposed to criminal third parties without their authorization.

31. Plaintiffs' claims arise out of the same common course of conduct giving rise to the claims of the other members of the Class.

32. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other members of the Class.

33. Plaintiffs are represented by counsel competent and experienced in the prosecution of consumer protection and tort litigation.

34. The questions of law and fact common to the members of the Class predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

35. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently,

and without the unnecessary duplication of evidence, effort, and expense of numerous individual actions. The benefits of proceeding as a class, including providing injured persons or entities with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any potential difficulties in managing this class action.

36. The prosecution of separate actions by individual members of the Class is not feasible and would create a risk of inconsistent or varying adjudications.

COUNT I
Negligence

37. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

38. Plaintiffs bring this claim on behalf of themselves and all members of the proposed Class against Defendant.

39. Defendant had and continues to have a duty to Plaintiffs and members of the Class to safeguard and protect their PII. Defendant created this duty by requiring Plaintiffs and members of the Class to provide their PII, storing the PII, using the PII for commercial gain, and making representations in its Privacy Policy that it uses "reasonable organizational, technical, and administrative measures designed to protect Personal Information within our organization."

40. Defendant's duty required it, among other things, to design and employ cybersecurity systems, anti-hacking technologies, intrusion detection and reporting systems, and employee training sufficient to protect the PII from unauthorized access and to promptly alert Defendant to any such access and enable it to determine the extent of any compromised PII.

41. Had Defendant adequately designed, employed, and maintained appropriate technological and other systems, as well as properly trained its employees to avoid email phishing scams and other potential causes of data breaches, the PII would not have been compromised or, at a minimum, Defendant would have known of the unauthorized access sooner and would be able to accurately inform Plaintiffs and the other members of the Class of the extent to which their PII had been compromised.

42. Defendant breached its duties of care by, among other things, failing to maintain appropriate technological and other systems to prevent unauthorized access, failing to properly train its employees to avoid email phishing scams and other potential causes of data breaches, failing to minimize the PII that any intrusion could compromise (i.e., less aggregation and weeding out unnecessary and stale data), and failing to provide timely notice to affected consumers with accurate information so that those affected could begin minimizing the impact of the incident.

43. Defendant's breach of its duties provided the means for third parties to access, obtain, and misuse the PII of Plaintiffs and the members of the Class without authorization. It was reasonably foreseeable that such breaches would expose the PII to criminals and other unauthorized users.

44. Defendant's breach of its duties has directly and proximately injured Plaintiffs and members of the Class including by foreseeably causing them to expend time and resources investigating the extent to which their PII had been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (now or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

45. Plaintiffs and the members of the Class are entitled to damages in an amount to be proven at trial, and to equitable relief, including injunctive relief.

COUNT II
Negligent Misrepresentation

46. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

47. Plaintiffs bring this claim on behalf of themselves and all members of the proposed Class against Defendant.

48. Defendant represented in its Privacy Policy that it uses "reasonable organizational, technical, and administrative measures designed to protect Personal Information within our organization."

49. These representations were for the express purpose of protecting Plaintiffs and Class members' PII, and created an affirmative duty to use "reasonable organizational, technical, and administrative measures designed to protect Personal Information."

50. Defendant made these representations in the ordinary course of its regular business with the intent to induce Plaintiffs and Class members to supply their PII to Defendant for the purposes of using Defendant's facilities or working for Defendant.

51. Defendant knew that Plaintiffs and Class members would rely on the above-referenced representations in supplying their PII to Defendant for the purposes of using Defendant's facilities or working for Defendant.

52. Plaintiffs and Class members justifiably relied on Defendant's representations regarding the security of their PII in choosing to provide their PII to Defendant.

53. Defendant violated these representations by failing to use reasonable measures to secure the PII of Plaintiffs and Class members. Specifically, Defendant failed to maintain appropriate technological and other systems to prevent unauthorized access, failed to properly train its employees to avoid email phishing scams and other potential causes of data breaches, failed to minimize the PII that any intrusion could compromise (i.e., less aggregation and weeding out unnecessary and stale data), and failed to provide timely notice to affected consumers with accurate information so that those affected could begin minimizing the impact of the incident.

54. It was reasonably foreseeable in that Defendant knew or should have known that its failure to implement reasonable measures to protect the PII of Plaintiffs and Class members would result in the data breach of such information.

55. The release and disclosure of Plaintiffs and Class members' PII to third parties was without Plaintiffs and Class members' authorization or consent.

56. Defendant's breach of its duties has directly and proximately injured Plaintiffs and members of the Class, including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and

taking reasonable steps (now or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

COUNT III
Negligence *Per Se* For Violation of the Federal Trade Commission Act, 15 U.S.C. § 45

57. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

58. Plaintiffs bring this claim on behalf of themselves and all members of the proposed Class against Defendant.

59. Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce." The FTC has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5.

60. The FTC has provided guidance on how businesses should protect against data breaches, including: protect the personal customer information they acquire; properly dispose of personal information that is not necessary to maintain; encrypt information stored on computer networks; understand their network's vulnerabilities; and install vendor-approved updates to address those vulnerabilities. FTC guidance also recommends that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and watch for large amounts of data being transmitted from the system.

61. Plaintiffs and members of the Class are within the class of persons Section 5 of the FTCA was intended to protect.

62. The harm that has occurred is the type of harm the FTCA was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and members of the Class

63. Defendant owed a duty to Plaintiffs and members of the Class under the Section 5 of the FTCA.

64. Defendant breached its duty under Section 5 of the FTCA by, among other things, failing to maintain appropriate technological and other systems to prevent unauthorized access, failing to properly train its employees to avoid email phishing scams and other potential causes of data breaches, failing to minimize the PII that any intrusion could compromise (i.e., less aggregation and weeding out unnecessary and stale data), and failing to provide timely notice to affected consumers with accurate information so that those affected could begin minimizing the impact of the incident.

65. Defendant's breach of its duties has directly and proximately injured Plaintiffs and members of the Class, including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (now or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

66. Plaintiffs and the members of the Class are entitled to damages in an amount to be proven at trial, and to equitable relief, including injunctive relief.

COUNT IV
Negligence *Per Se* For Violation of the Nevada Data Breach Law, NRS §§ 603A.010, *et seq.*

67. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

68. Plaintiffs bring this claim on behalf of themselves and all members of the proposed Class against Defendant.

69. Defendant suffered a "breach of the security of the system data" as defined in NRS § 603A.020.

70. Defendant is a "data collector" as defined in NRS § 603A.030.

71. The data breach involved "personal information" as defined in NRS § 603A.040.

72. Pursuant to the Nevada Data Breach Law ("NDBL"), NRS §§ 603A.010, *et seq.*, "A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from

unauthorized access, acquisition, destruction, use, modification or disclosure." NRS § 603A.210(1).

73. Further, a data collector must, "in the most expedient time possible and without unreasonable delay," "disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." NRS § 603A.220(1).

74. Plaintiffs and members of the Class are within the class of persons the NDBL was intended to protect.

75. The harm that has occurred is the type of harm the NDBL was intended to guard against.

76. Defendant owed a duty to Plaintiffs and members of the Class under the NDBL.

77. Defendant breached its duty under NDBL by, among other things, failing to maintain appropriate technological and other systems to prevent unauthorized access, failing to properly train its employees to avoid email phishing scams and other potential causes of data breaches, failing to minimize the PII that any intrusion could compromise (i.e., less aggregation and weeding out unnecessary and stale data), and failing to provide timely notice to affected consumers with accurate information so that those affected could begin minimizing the impact of the incident.

78. Defendant's breach of its duties has directly and proximately injured Plaintiffs and members of the Class, including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (now or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

79. Plaintiffs and the members of the Class are entitled to damages in an amount to be proven at trial, and to equitable relief, including injunctive relief.

COUNT V
Breach of Contract

80. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

81. Plaintiffs bring this claim on behalf of themselves and all members of the proposed Class against Defendant.

82. Defendant entered into contracts with Plaintiffs and Class members to provide access to its casinos or employment opportunities.

83. These contracts included or otherwise incorporated Defendant's Privacy Policy, in which Defendant represented that it uses "reasonable organizational, technical, and administrative measures designed to protect Personal Information within our organization."

84. Defendant has breached these contracts by failing to use "reasonable organizational, technical, and administrative measures designed to protect Personal Information within our organization," including by failing to maintain appropriate technological and other systems to prevent unauthorized access, failing to properly train its employees to avoid email phishing scams and other potential causes of data breaches, failing to minimize the PII that any intrusion could compromise (i.e., less aggregation and weeding out unnecessary and stale data), and failed to provide timely notice to affected consumers with accurate information so that those affected could begin minimizing the impact of the incident.

85. Plaintiffs and Class members have suffered damages as a result of Defendant's breach, including through identity theft and expenses incurred combating identity theft.

COUNT VI
Violation Of The Nevada Deceptive Trade Practices Act,
NRS § 598.0903, *et seq.*

86. Plaintiffs incorporate by reference the allegations in the preceding paragraphs as if fully set forth herein.

87. Plaintiffs bring this claim on behalf of themselves and all members of the proposed Class against Defendant.

88. Based on the foregoing allegations, Defendant has violated the following provisions of the Nevada Deceptive Trade Practices Act ("NDTPA"), NRS §§ 598.0903, *et seq*:

(a) Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale. NRS § 598.0915(5);

(b) Representing that goods or services for sale are of a particular standard, quality, or grade when Defendant knew or should have known that they are of another standard, quality, or grade. NRS § 598.0915(7);

(c) Advertising goods or services with intent not to sell them as advertised. NRS § 598.0915(9);

(d) Failing to disclose a material fact in connection with the sale of goods or services. NRS § 598.0923(2);

(e) Violating a state or federal statute or regulation relating to the sale or lease of goods or services. NRS § 598.0923(3)

89. Defendant breached these provisions by requiring Plaintiffs and members of the Class to provide PII without disclosing or otherwise representing that Defendant, among other things, failed to maintain appropriate technological and other systems to prevent unauthorized access, failed to properly train its employees to avoid email phishing scams and other potential causes of data breaches, failed to minimize the PII that any intrusion could compromise (i.e., less aggregation and weeding out unnecessary and stale data), and would fail to provide timely notice to affected consumers with accurate information so that those affected could begin minimizing the impact of the incident.

90. Defendant also breached these provisions by making false representations regarding the security of the PII of Plaintiffs and Class members. Specifically, Defendant represented in its Privacy Policy that it uses "reasonable organizational, technical, and administrative measures designed to protect Personal Information within our organization." But these representations were false because Defendant failed to maintain appropriate technological and other systems to prevent unauthorized access, failed to properly train its employees to avoid email phishing scams and other potential causes of data breaches, failed to minimize the PII that

any intrusion could compromise (i.e., less aggregation and weeding out unnecessary and stale data), and failed to provide timely notice to affected consumers with accurate information so that those affected could begin minimizing the impact of the incident.

91. 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 the PII of Plaintiffs and members of the Class.

92. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and members of the Class have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary 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 PII.

93. Plaintiffs and other members of the Class are entitled to seek action against Defendant under the NDTPA. NRS § 41.600(2)(e).

94. Plaintiffs and the members of the Class are entitled to actual damages in an amount to be determined at trial, punitive damages, equitable relief, and reasonable costs and attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) An Order certifying the proposed Class, and appointing Plaintiffs and their Counsel to represent the Class;

(b) An Order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs and the Class' PII;

(c) An Order compelling Defendant to employ and maintain appropriate systems and policies to protect consumer PII and to promptly detect, and timely and accurately report, any unauthorized access to that data;

(d) An award of compensatory, statutory, and punitive damages, in an amount to be determined;

(e) An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law;

(f) Interest on all amounts awarded, as allowed by law; and

(g) Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: July 2, 2020

Respectfully submitted,

/s/ Don Springmeyer

WOLF, RIFKIN, SHAPIRO, SCHULMAN AND RABKIN, LLP
Don Springmeyer, Esq. (SBN 1021)
Daniel Bravo, Esq. (SBN 13078)
A. Jill Guingcangco, Esq. (SBN 14717)
3556 E Russell Rd, Second Floor
Las Vegas, Nevada 89120
Telephone: (702) 341-5200 / Fax: (702) 341-5300
Email: dspringmeyer@wrslawyers.com
Email: dbravo@wrslawyers.com
Email: ajg@wrslawyers.com

BURSOR & FISHER, P.A.
Yitzchak Kopel (*Pro Hac Vice Forthcoming*)
Max S. Roberts (*Pro Hac Vice*)
888 Seventh Avenue, Third Floor
New York, NY 10019
Telephone: (646) 837-7150 / Fax: (212) 989-9163
Email: ykopel@bursor.com
Email: mroberts@bursor.com

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on this 2nd day of July, 2020, a true and correct copy of **FIRST AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND** was served via the United States District Court CM/ECF system on all parties or persons requiring notice.

By */s/ Christie Rehfeld*
Christie Rehfeld, an Employee of
WOLF, RIFKIN, SHAPIRO, SCHULMAN & RABKIN, LLP