Seth Bayles, Nevada Bar No. 15700
seth@bayleslawgroup.net
BAYLES LAW GROUP, PLLC
10175 W. Twain Ave., Suite 130
Las Vegas, NV 89147
Telephone: (702) 268-9987

Thiago M. Coelho, SBN 324715
thiago@wilshirelawfirm. com
Carolin K. Shining, SBN 201140
cshining@wilshirelawfirm.com
Jennifer M. Leinbach, SBN 281404
jleinbach@wilshirelawfirm.com
Jesenia Martinez, SBN 316969
jesenia.martinez@wilshirelawfirm.com
Jesse S. Chen, SBN 336294
jchen@wilshirelawfirm.com
WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

Attorneys for Plaintiffs and Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

FERNANDO MENDOZA and SOPHIA MENDOZA, individually and on behalf of all others similarly situated, Plaintiffs, v. CRYSTAL BAY CASINO, LLC a Nevada limited liability company, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs FERNANDO MENDOZA and SOPHIA MENDOZA ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant CRYSTAL BAY CASINO, LLC ("CBC" or "Defendant") based upon personal knowledge as to themselves and their own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigations of their attorneys.

NATURE OF THE ACTION

1. On or around November 27, 2022, CBC had their data servers breached by unauthorized third-party hackers, who stole the highly sensitive personal information—including, *inter alia*, the names, driver's license numbers, and Social Security numbers—of approximately 86,291 individuals across the United States.[1]

2. CBC is a resort and casino located in the Lake Tahoe area, on the Nevada side the California-Nevada border. CBC offers a membership program to its customers named the "Player's Club," which provides members with certain benefits such earning points towards certain rewards, preferred parking, access to certain promotions, and eligibility to win certain prizes. CBC requires an individual to provide their full name and a copy of a valid, government-issued photo identification, among other sensitive personal information, in order to become a member of the Player's Club.[2] As a result, CBC collects and stores the PII of tens of thousands of customers across the country.

3. Under statute and regulation, CBC had a duty to implement reasonable, adequate industry-standard data security policies safeguards to protect its customers' PII. CBC failed to do so and, as a result, its customers' sensitive information was accessed and misused by unauthorized third-party hackers.

4. Plaintiffs, individually and on behalf of those similarly situated persons (hereafter "Class Members"), bring this class action to secure redress against CBC for its reckless and

[1] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/46950cd6-3847-4f0b-b019-3cf7c17b7333.shtml (last visited March 6, 2023).

[2] "Player's Club" https://www.crystalbaycasino.com/gaming/players-club/ (last accessed March 6, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

negligent violation of their privacy rights. Plaintiffs and Class Members are customers of CBC who had their PII collected, stored and ultimately breached by CBC.

5. Plaintiffs and Class Members have suffered injuries and damages. As a result of CBC's wrongful actions and inactions, Plaintiffs and Class Members' PII—including, *inter alia*, their names, drivers' license numbers, and Social Security numbers—have all been compromised. Plaintiffs and Class Members have had their privacy rights violated and are now exposed to a heightened risk of identity theft and credit fraud for the remainder of their lifetimes. Plaintiffs and Class Members must now spend time and money on prophylactic measures, such as increased monitoring of their personal and financial accounts and the purchase of credit monitoring services, to protect themselves from future loss. Further, Plaintiffs and Class Members have lost the value of their PII, which have determinable market value on both legitimate and dark web marketplaces. Finally, Plaintiffs and Class Members have lost the benefit of their bargain, as they would not have purchased CBC's services, or would have paid substantially less for them, had they been aware that CBC would not implement reasonable and adequate safeguards to protect their PII.

6. Further, CBC unreasonably delayed in notifying Plaintiffs and Class Members of the data breach. Despite having discovered the breach on November 27, 2022, CBC did not begin notifying Plaintiffs and Class Members until on or around February 24, 2023.[3] CBC's notice provides no justification as to why it chose to wait eighty-nine days to notify Plaintiffs and Class Members of the imminent harm that they placed them under by breaching their PII.

7. As a result of CBC's wrongful actions and inactions, patient information was stolen. Plaintiffs and Class Members who have had their PII compromised by nefarious third-party hackers, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages. Plaintiffs and Class Members bring this action to secure redress against CBC.

[3] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/46950cd6-3847-4f0b-b019-3cf7c17b7333.shtml (last visited March 6, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

THE PARTIES

8. Plaintiff Fernando Mendoza is a Nevada citizen residing in Reno, Nevada. Plaintiff is a former customer and employee of CBC. In or around 2017 or 2018, Plaintiff Fernando Mendoza signed up for a membership to Defendant's Player's Club, during the process of which he provided his sensitive PII to Defendant. Plaintiff also provided his sensitive PII to Defendant in connection to his employment with Defendant, which ended in 2018. On or around February 24, 2023, Plaintiff Fernando received a data breach notice from CBC informing him that his personal information, including, *inter alia*, his name, driver's license number, and Social Security number, had been implicated in the data breach.

9. Plaintiff Sophia Mendoza is a Nevada citizen residing in Reno, Nevada. Plaintiff Sophia Mendoza is a former customer of CBC. In or around 2017 or 2018, Plaintiff Sophia signed up for a membership to Defendant's Player's Club, during the process of which she provided her sensitive PII to Defendant. On or around February 24, 2023, Plaintiff Sophia received a data breach notice from CBC informing her that her personal information, including, *inter alia*, her name and her driver's license number had been implicated in the data breach.

10. Defendant Crystal Bay Casino, LLC is a Nevada limited liability company with its principal place of business at 14 NV-28, Crystal Bay, Nevada 89402. Defendant's Manager is Roger William Norman, who is a Nevada citizen residing in Reno, Nevada. CBC's registered agent for service of process is Sierra Corporate Services – Reno, which is located at 100 West Liberty Street 10th Floor, Reno, Nevada, 89501.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over the claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). As of the original filing of this Complaint, there exist members of the putative Plaintiff class that are domiciled across the United States. This evidenced by the fact that Defendant's data breach has impacted at least 500

California residents[4], 423 Massachusetts residents[5], and 54 Maine residents[6], among others. Further, there are more than 100 putative class members, and the amount in controversy exceeds $5 million.

12. The Court also has personal jurisdiction over the Parties because Defendant is a citizen of Nevada, routinely conducts business in Nevada and has sufficient minimum contacts in Nevada to have intentionally availed themselves to this jurisdiction.

13. Venue is proper in this District because, among other things: (a) Plaintiffs Fernando and Sophia Mendoza reside in this District and are citizens of this State; (b) Defendant resides in and directed its activities at residents in this District; and (c) many of the acts and omissions that give rise to this Action took place in this judicial District for services provided in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

14. Defendant Crystal Bay Casino is a resort and casino located in the Lake Tahoe area, on the Nevada side the California-Nevada border. CBC offers a membership known as the Player's Club to its customers, wherein its customers can earn points towards rewards and access certain exclusive resort benefits. As a requirement to obtain membership to the Player's Club, CBC requires its customers to provide it with their sensitive PII, including, *inter alia*, their full names and a form of valid, government-issued photo identification.

15. At the same time, Defendant CBC also employs individuals to provide services to its customers. CBC requires those employees to provide their sensitive PII, including, *inter alia*, their Social Security numbers, to CBC in order to obtain such employment.

[4] Data Breach Notifications, Office of the California Attorney General, https://oag.ca.gov/ecrime/databreach/reports/sb24-563594 (last accessed March 6, 2023).

[5] "Data Breach Report 2023" https://www.mass.gov/doc/data-breach-report-2023/download (last accessed March 6, 2023).

[6] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/46950cd6-3847-4f0b-b019-3cf7c17b7333.shtml (last visited March 6, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

16. Defendant CBC stores the sensitive PII it obtains from its customers and employees in its internal data servers.

17. On or around November 27, 2022, CBC's systems were accessed by unauthorized third-party hackers, who exfiltrated Plaintiffs' and Class Members' sensitive PII—including, but not limited to, their names, driver's license numbers, and Social Security Numbers. This breach implicated the sensitive PII that CBC had collected, recorded, and stored in its internal data servers for both its Players' Club members and its' employees. In its data breach notification filed the Office of the Maine Attorney General, CBC reported that the data breach had affected 86, 291 individuals.[7]

B. CBC's Unreasonably Delayed and Inadequate Notification

18. CBC owed Plaintiffs and Class Members a duty under state law to provide timely notification of the data breach. Under Nev. Rev. Stat. §603A.220, CBC was required to provide such notification "in the most expedient time possible and without unreasonable delay."

19. In its Data Breach Notice sent to Plaintiffs, CBC claims that it discovered unusual activity on its data servers in November of 2022. Specifically, CBC claims that it had discovered that certain files had been copied from its data systems on November 27, 2022. However, CBC did not begin notifying Plaintiffs and Class Members of this security breach until on or around February 24, 2023, at least eighty-nine days later.

20. CBC has provided no reason or justification as to why it delayed in notifying Plaintiffs and Class Members for almost *three* months after it became apparent that its data systems had been breached and copied. CBC's data breach notification was not made in the most expedient time possible and was unreasonably delayed, in violation of Nev. Rev. Stat. §603A.220.

21. CBC's violation of Nev. Rev. Stat. §603A.220 constitutes a deceptive trade practice under the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§598.0903, *et seq*. Nev. Rev. Stat. §603A.260.

[7] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/46950cd6-3847-4f0b-b019-3cf7c17b7333.shtml (last visited March 6, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

C. CBC's Obligation to Protect Customer and Employee PII Under State and Federal Law

22. Under Nev. Rev. Stat. §603A.210, CBC, as a corporation that collects nonpublic personal information and records it, was required to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure." Upon information and belief, CBC failed to implement such reasonable security measures to protect the sensitive PII entrusted to it by its customers and employees, and instead allows it to be accessed, disclosed, and used by unauthorized third-party hackers, in violation of this statute.

23. CBC's violation of Nev. Rev. Stat. §603A.210 constitutes a deceptive trade practice under the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§598.0903, *et seq*. Nev. Rev. Stat. §603A.260.

24. Further, the Federal Trade Commission Act, 15 U.S.C. §45 prohibits CBC from engaging in "unfair or deceptive acts or practices affecting commerce." The Federal Trade Commission has found The Federal Trade Commission has found that a company's failure to maintain reasonable and appropriate data security for the consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3rd Cir. 2015).

25. CBC failed to comply with each of these state and federal statutes by failing to implement and maintain reasonable security procedures to protect Plaintiffs and Class Members' PII.

D. Applicable Standards of Care

26. In addition to their obligations under state and federal law, CBC owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. CBC owed a duty to Plaintiffs and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer system and networks, and the personnel

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

responsible for them, adequately protected the PII of Plaintiffs and Class Members.

27. CBC owed a duty to Plaintiffs and the Class Members to design, maintain, and test their computer system to ensure that the PII in CBCs' possession was adequately secured and protected.

28. CBC owed a duty to Plaintiffs and the Class Members to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training their employees and others who accessed the PII in their possession, including adequately training their employees and others who accessed PII in their computer systems on how to adequately protect PII.

29. CBC owed a duty of care to Plaintiffs and Class Members to implement processes that would detect a breach of their data security systems in a timely manner.

30. CBC owed a duty to Plaintiffs and the Class Members to act upon data security warnings and alerts in a timely fashion.

31. CBC owed a duty to Plaintiffs and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to provide or entrust their PII to CBC.

32. CBC owed a duty to Plaintiffs and the Class Members to disclose in a timely and accurate manner when the data breach occurred.

33. CBC owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. CBC received PII from Plaintiffs and Class Members with the understanding that Plaintiffs and Class Members expected their PII to be protected from disclosure. CBCs knew that a breach of its data systems would cause Plaintiffs and Class Members to incur damages.

E. Stolen Information Is Valuable to Hackers and Thieves

34. It is well known, and the subject of many media reports, that PII is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation and frequent public

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

announcements of data breaches, CBC opted to maintain an insufficient and inadequate system to protect the PII of Plaintiffs and Class Members.

35. Plaintiffs and Class Members value their PII, as in today's electronic-centric world, their PII is required for numerous activities, such as new registrations to websites, or opening a new bank account, as well as signing up for special deals.

36. Legitimate organizations and criminal underground alike recognize the value of PII. That is why they aggressively seek and pay for it.

37. PII is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as "dumps." *See All About Fraud: How Crooks Get the CVV*, Krebs on Security (April 26, 2016), https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/.

38. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

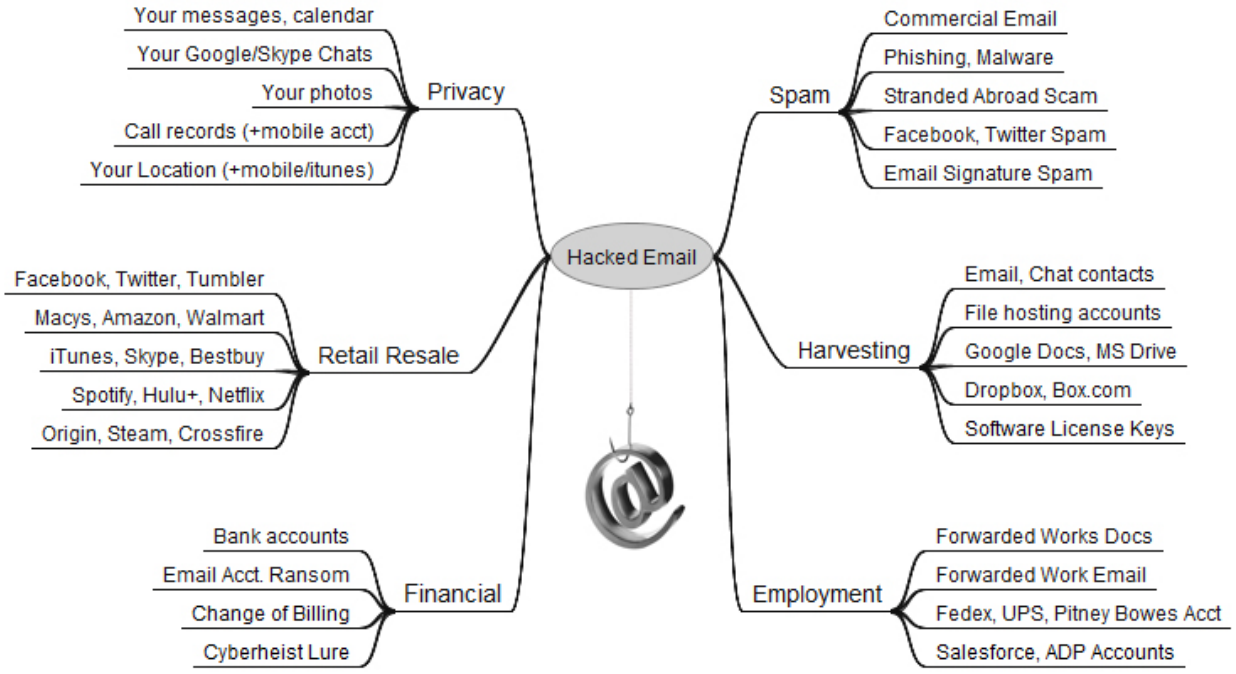
39. In addition to PII, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.[8]

40. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.[9]

[8] *Identity Theft and the Value of Your Personal Data*, Trend Micro (Apr. 30, 2015), https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data. (last accessed March 6, 2023).

[9] Brian Krebs, *The Value of a Hacked Email Account*, Krebs on Security (June 13, 2013, 3:14 PM), https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/. (last accessed March 6, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137



41. Hacked information can also enable thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers."[10]

F. The Data Breach Has and Will Result in Additional Identity Theft and Identity Fraud

42. CBC failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiffs and the Class Members. The ramification of CBC's failure to keep Plaintiffs and the Class Members' data secure is severe.

[10] *Report on Phishing* (Oct. 2006), https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf (last accessed March 6, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

43. Between 2005 and 2019, at least 249 million individuals were affected by health care data breaches.[11] In 2019 alone, over 505 data HIPAA data breaches were reported, resulting in over 41 million healthcare records being exposed, stolen, or unlawfully disclosed.[12]

44. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." *See Victims of Identity Theft*, U.S. Department of Justice (Dec 2013), https://www.bjs.gov/ content/pub/pdf/vit12.pdf. In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*.

G. Annual Monetary Losses from Identity Theft are in the Billions of Dollars

45. Javelin Strategy and Research reports that losses from identity theft reached $21 billion in 2013. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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.

See GAO, Report to Congressional Requesters (June 2007), http://www.gao.gov/new.items/d07737.pdf. (last accessed March 6, 2023).

46. This is particularly the case with HIPAA data breaches such as CBC's, as the information implicated, such as social security numbers of medical history, cannot be changed. Once such information is breached, malicious actors can continue misusing the stolen information

[11] *Healthcare Data Breaches: Insights and Implications*, National Library of Medicine (May 13, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133. (last accessed March 6, 2023).

[12] *December 2019 Healthcare Data Breach*, HIPAA Journal, https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed March 6, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

for years to come. Indeed, medical identity theft are one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.[13] Victims of medical identity theft "often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[14]

47. Indeed, a study by Experian found that the average total cost of medical identity theft is "nearly $13,500" per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.[15] Victims of healthcare data breaches often find themselves "being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores."[16]

48. Plaintiffs and the Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any financial or identity fraud they suffer.

H. Plaintiffs and Class Members Suffered Damages

49. The exposure of Plaintiffs and Class Members' PII to unauthorized third-party hackers was a direct and proximate result of CBCs' failure to properly safeguard and protect Plaintiffs and Class Members' PII from unauthorized access, use, and disclosure, as required by and state and federal law. The data breach was also a result of CBC's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, as required by state and federal law.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

[13] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare* (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/. (last accessed March 6, 2023).
[14] *Id.*
[15] *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/ healthcare -data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed March 6, 2023).
[16] *Id.*

50. Plaintiffs and Class Members' PII is private and sensitive in nature and was inadequately protected by CBC. CBC did not obtain Plaintiffs and Class Members' consent to disclose their PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

51. As a direct and proximate result of CBC's wrongful actions and inaction and the resulting data breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, paying for credit and identity monitoring services, spending time on credit and identity monitoring, placing "freezes" and "alerts" with credit reporting agencies, contacting their personal, financial and healthcare institutions, closing or modifying personal, financial or healthcare accounts, and closely reviewing and monitoring their credit reports, financial accounts and healthcare accounts for unauthorized activity.

52. Plaintiffs has also lost the value of her PII. PII is a valuable commodity, as evidenced by numerous companies which purchase PII from consumers, such as UBDI, which allows its users to link applications like Spotify, Twitter, or Apple Health and opt-in to paid opportunities to earn income, and Brave, which uses a similar business model, and by market-based pricing data involving the sale of stolen PII across multiple different illicit websites.

53. Top10VPN, a secure network provider, has compiled pricing information for stolen PII, including $160.15 for online banking details, $35.00 for credit reports, and $62.61 for passports. Standalone Yahoo email accounts have been listed for as little as $0.41, while banking logins are in the range of $500, and verified Paypal accounts with high balances are listed at as much as $2,000.

54. In addition, Privacy Affairs, a cyber security research firm, has listed the following prices for stolen PII:

U.S. driving license, high quality:	$550
Auto insurance card:	$70
AAA emergency road service membership card:	$70

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Wells Fargo bank statement:	$25
Wells Fargo bank statement with transactions:	$80
Rutgers State University student ID:	$70

55. CBCs' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure and theft of their PII;

b. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII being exposed to and misused by unauthorized third-party hackers;

c. The untimely and inadequate notification of the data breach;

d. 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; and

e. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market.

CLASS ACTION ALLEGATIONS

56. Plaintiffs brings this action on their own behalf and pursuant to the Federal Rules of Civil Procedure Rule 23(a), (b)(2), (b)(3), and (c)(4). Plaintiffs intends to seek certification of a Nationwide Class and California Subclass. The Classes are initially defined as follows:

The Nationwide Class, initially defined as:

> All persons residing in the United States of America who received a data breach notice informing them that their PII had been breached by unauthorized third parties as a result of the data breach announced by Crystal Bay Casino, LLC.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

The Nevada Sub-Class, initially defined as:

> All persons residing in the State of Nevada who received a data breach notice informing them that their PII had been breached by unauthorized third parties as a result of the data breach announced by Crystal Bay Casino, LLC.

57. Excluded from each of the above Classes is Defendant, including any entity in which CBC has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judge and the court personnel in this case and any members of their immediate families. Plaintiffs reserves the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded or otherwise modified.

58. *Numerosity*, Fed. R. Civ. P. 23(a)(1): The members of the Classes are so numerous that the joinder of all members is impractical. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control, such as reservation receipts and confirmations.

59. *Commonality*, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;

b. Whether Defendant violated common and statutory by failing to implement reasonable security procedures and practices;

c. Which security procedures and which data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

d. Whether Defendant knew or should have known of the security breach prior to the disclosure;

e. Whether Defendant has complied with any implied contractual obligation to use reasonable security measures;

f. Whether Defendant acts and omissions described herein give rise to a claim of negligence;

g. Whether Defendant knew or should have known of the security breach prior to its disclosure;

h. Whether Defendant had a duty to promptly notify Plaintiffs and Class Members that their PII was, or potentially could be, compromised;

i. What security measures, if any, must be implemented by Defendant to comply with its duties under state and federal law;

j. The nature of the relief, including equitable relief, to which Plaintiffs and the Class Members are entitled; and

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

60. *Typicality*. Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because Plaintiffs are former customers and employees of Defendant who had their PII breached by Defendant.

61. *Adequacy of Representation*, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiffs has retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiffs intends to prosecute this action vigorously. Plaintiffs' claims are typical of the claims of other members of the Classes and Plaintiffs has the same non-conflicting interests as the other Class Members. Therefore, the interests of the Classes will be fairly and adequately represented by Plaintiffs and their counsel.

62. *Superiority of Class Action*, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

all the members of the Classes is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

63. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied.

64. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Negligence

(On Behalf of Plaintiffs and the Nationwide Class)

65. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 64, inclusive, of this Complaint as if set forth fully herein.

66. In 2016, the Federal Trade Commission ("FTC") updated its publication, "Protecting Personal Information: A Guide for Business," which establishes guidelines for fundamental data security principles and practices for business. [17] Among other things, the guidelines dictate businesses should protect any personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses implement an intrusion detection system to expose breaches as soon as they occur; monitor all incoming traffic for

[17] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf. (last accessed March 6, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

activity indicating someone is attempting to infiltrate or hack the system; monitor instances when large amounts of data are transmitted to or from the system; and have a response plan ready in the event of a breach. [18] Additionally, the FTC recommends that companies 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. [19]

67. Defendant owed Plaintiffs and the Class Members a duty of care in the handling of customers' PII. This duty included, but was not limited to, keeping that PII secure and preventing disclosure of the PII to any unauthorized third parties. This duty of care existed independently of Defendants' contractual duties to Plaintiffs and the Class Members. Under the FTC Guidelines, and other sources of industry-wide cybersecurity standards, Defendant is obligated to incorporate adequate measures to safeguard and protect PII that is entrusted to them in their ordinary course of business and transactions with customers.

68. Pursuant to Nev. Rev. Stat. §603A.210, CBC, as a corporation that collects nonpublic personal information and records it, was required to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."

69. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' PII. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the businesses' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders from these actions further clarify the measures

[18] *Id*.

[19] Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf. (last accessed March 6, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

businesses are required to undertake in order to satisfy their data security obligations. [20]

70. Additional industry guidelines which provide a standard of care can be found in the National Institute of Standards and Technology's ("NIST's") *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018), https://nvlpubs. nist. gov/nistpubs/CSWP/ NIST. CSWP. 04162018. pdf. Among other guideposts, the NIST's framework identifies seven steps for establishing or improving a cybersecurity program (section 3. 2). Those steps are:

> *Step 1: Prioritize and Scope*. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.
>
> *Step 2: Orient*. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.
>
> *Step 3: Create a Current Profile*. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.
>
> *Step 4: Conduct a Risk Assessment*. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.
>
> *Step 5: Create a Target Profile*. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and

[20] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-securityenforcement ((last accessed March 6, 2023).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

71. In addition to their obligations under federal regulations and industry standards, Defendant owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiffs and the Class Members.

72. Defendant owed a duty to Plaintiffs and the Class Members to design, maintain, and test their internal data systems to ensure that the PII in DEFENDANT's possession was adequately secured and protected.

73. Defendant owed a duty to Plaintiffs and the Class Members to create and implement reasonable data security practices and procedures to protect the PII in its custodianship, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

74. Defendant owed a duty to Plaintiffs and the Class Members to implement processes or safeguards that would detect a breach of their data security systems in a timely

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

manner.

75. Defendant owed a duty to Plaintiffs and the Class Members to act upon data security warnings and alerts in a timely fashion.

76. Defendant owed a duty to Plaintiffs and the Class Members to timely disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material consideration in Plaintiffs and Class Members' decisions to entrust their PII to Defendant.

77. Defendant owed a duty to Plaintiffs and the Class Members to disclose in a timely and accurate manner when data breaches occur.

78. Defendant owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices and systems. Defendant collected PII from Plaintiffs and the Class Members. Defendant knew that a breach of its data systems would cause Plaintiffs and the Class Members to incur damages.

79. Defendant breached its duties of care to safeguard and protect the PII which Plaintiffs and the Class Members entrusted to it. Defendant adopted inadequate safeguards to protect the PII and failed to adopt industry-wide standards set forth above in its supposed protection of the PII. Defendant failed to design, maintain, and test its computer system to ensure that the PII was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of its data security systems in a timely manner, failed to disclose the breach to potentially affected customers in a timely and comprehensive manner, and otherwise breached each of the above duties of care by implementing careless security procedures which led directly to the breach.

80. Defendant breached the duties set forth in 15 U.S.C. §45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. §45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiffs and Class Member's PII. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information that it keeps; failed to properly dispose of personal information that was no longer needed; failed

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

to encrypt information stored on computer networks; lacked the requisite understanding of their network's vulnerabilities; and failed to implement policies to correct security problems. In violation of the NIST's Framework, Defendant, *inter alia*, failed to adopt sufficient resources to identity and address security gaps.

81. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

82. As a direct and proximate result of Defendant's failure to adequately protect and safeguard the PII, Plaintiffs and the Class members suffered damages. Plaintiffs and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiffs and the Class members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiffs and Class Members of the data breach until weeks had passed. In addition, Plaintiffs and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

83. Plaintiffs and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

SECOND CAUSE OF ACTION

Quasi-Contract/Unjust Enrichment

(On Behalf of Plaintiffs and the Nationwide Class)

84. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 83, inclusive, of this Complaint as if set forth fully herein.

85. Plaintiffs and Class Members provided their PII and conferred a monetary benefit upon Defendant in exchange for services and employment. Plaintiffs and Class Members did so under the reasonable but mistaken belief that part of their monetary payment to Defendant would cover the implementation of reasonable, adequate, and statutorily mandated safeguards to protect their PII. Defendant was enriched when it sold its services at a higher price than it otherwise

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

would have based on those reasonable but mistaken beliefs.

86. Defendant's enrichment came at the expense of Plaintiffs and Class Members, who would not have paid for Defendant's services, or would have only been willing to paid substantially less for them, had they been aware that Defendant had not implement reasonable, adequate and statutorily mandated safeguards to protect their PII.

87. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members suffered have suffered damages in the form of their lost benefit of the bargains. Plaintiffs and Class Members entered into agreements with Defendant under the reasonable but mistaken belief that it would reasonably and adequately protect their PII. Plaintiffs and Class Members would not have entered into such agreements had they known that Defendant would not reasonably and adequately protect their PII. Plaintiffs and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the services that include reasonable and adequate data security that they bargained for, and the services that do not that they actually received.

88. Defendant should not be permitted to retain Plaintiffs' and Class Members' lost benefits, without having adequately implemented the data privacy and security procedures for itself that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards. Defendant should not be allowed to benefit at the expense of consumers who trust Defendant to protect the PII that they are required to provide to Defendant in order to receive Defendant's services.

89. As a direct and proximate result of Defendants' fraudulent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

THIRD CAUSE OF ACTION

Breach of Fiduciary Duty

(On Behalf of Plaintiffs and the Nationwide Class)

90. Plaintiffs repeat and incorporate by reference each and every allegation contained in paragraphs 1 through 89 inclusive of this Complaint as if set forth fully herein.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

91. Plaintiffs and Class Members provided their PII to Defendant in confidence and under the reasonable but mistaken belief that Defendant would protect the confidentiality of that information. Plaintiffs and Class Members would not have provided Defendant with their PII had they known that Defendant would not take reasonable and adequate steps to protect it.

92. Defendant's acceptance and storage of Plaintiffs' and Class Members' PII created a fiduciary relationship between Defendant and Plaintiffs and Class Members. As a fiduciary of Plaintiffs and Class Members, Defendant has duty to act primarily for the benefit of its patients and health plan participants, which includes implementing reasonable, adequate, and statutorily complaint safeguards to protect Plaintiffs' and Class Members' PII.

93. Defendant breached its fiduciary duties to Plaintiffs and Class Members by, *inter alia,* failing to implement reasonable and adequate data security protections, failing to comply with the data security guidelines set forth by the FTC, NIST and HIPAA, failing to implement reasonable and adequate data security training for its employees, and otherwise failing to reasonably and adequately safeguard the PII of Plaintiffs and Class Members.

94. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered damages. Plaintiffs and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiffs and the Class Members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiffs and Class Members of the data breach until weeks had passed. In addition, Plaintiffs and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

95. As a direct and proximate result of Defendants' fraudulent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

FOURTH CAUSE OF ACTION

Violation of the Nevada Deceptive Trade Practices Act ("NDTPA")

Nev. Rev. Stat. Ann. §§598.0903, *et seq.*

(On behalf of Plaintiffs and the Nevada Sub-Class)

96. Plaintiffs repeat and incorporate by reference each and every allegation contained in paragraphs 1 through 95 inclusive of this Complaint as if set forth fully herein.

97. Defendant failed to "implement and maintain reasonable security measures" to protect Plaintiffs' and Class Members' sensitive PII, as required of it under Nev. Rev. Stat. §603A.210. Defendant's failure to implement and maintain such reasonable security measures is evidenced by the fact that they allowed Plaintiffs' and Class Members' sensitive PII to be accessed and exfiltrated by unauthorized third-party hackers.

98. Defendant's violation of Nev. Rev. Stat. §603A.210 constitutes a deceptive trade practice under the NDTPA. Nev. Rev. Stat. §603A.260.

99. Further, Defendant failed to provide Plaintiffs and Class Members notification of the data breach in the most expedient time possible and without unreasonable delay, in violation of §603A.220. Despite learning of the data breach in November of 2022, and specifically learning that files had been copied from its data servers on November 27, 2022, Defendant delayed notifying Plaintiffs and Class Members of the data breach until on or around February 24, 2022—approximately eighty-nine days later. Defendant has provided no reason or justification for this delay.

100. Defendant's violation of Nev. Rev. Stat. §603A.220 further constitutes a deceptive trade practice under the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§598.0903, *et seq*. Nev. Rev. Stat. §603A.260.

101. Defendant's violations were material to consumers, such as Plaintiffs and Class Members. Had Plaintiffs and Class Members known that Defendant would not implement reasonable and adequate data security safeguards to protect their PII, and that Defendant would not notify them of a data breach that had occurred within an expedient and timely manner, they would not have purchased Defendants' services, or would have paid substantially less for them.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

102. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiffs and Nevada Sub-Class members have suffered and will continue to suffer injury, including, *inter alia*, the loss of value of their PII, lost time and money spent dealing with the fallout of the data breach, and the lost benefit of their bargain. Plaintiffs and Nevada Sub-Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all of the Class Members, respectfully requests that the Court enter judgment in their favor and against Defendant as follows:

1. For an Order certifying the Classes as defined herein and appointing Plaintiffs and their Counsel to represent the Classes;
2. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;
3. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of PII compromised.
4. For an award of actual damages, statutory damages, and compensatory damages, in an amount to be determined at trial;
5. For an award of punitive and treble damages, in an amount to be determined at trial;
6. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and
7. For such other and further relief as this Court may deem just and proper.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: March 6, 2023

Respectfully Submitted,

/s/ *Seth Bayles*
Seth Bayles, Nevada Bar No. 15700
BAYLES LAW GROUP, PLLC
Attorneys for Plaintiffs

/s/ *Thiago M. Coelho*
Thiago M. Coelho*
**pro hac vice forthcoming*
WILSHIRE LAW FIRM, PLC
Attorneys for Plaintiffs

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

ClassAction.org
