Exhibit A

Thiago M. Coelho, *pro hac vice*
thiago@wilshirelawfirm.com
Jennifer M. Leinbach, CA SBN 281404
jleinbach@wilshirelawfirm.com
Jesenia Martinez, CA SBN 316969
jesenia.martinez@wilshirelawfirm.com
Jesse S. Chen, CA 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

David K. Lietz, *pro hac vice*
dlietz@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877

Attorneys for Plaintiffs and Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

FERNANDO MENDOZA, SOPHIA MENDOZA, and HUEY NGUYEN, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CRYSTAL BAY CASINO, LLC, a Nevada limited liability company,

Defendant.

Case No.: 3:23-CV-00092

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs FERNANDO MENDOZA, SOPHIA MENDOZA and HUEY NGUYEN ("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 of 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' and/or employees' PII. In particular, the PII was maintained on CBC's computer network in a condition vulnerable to cyberattacks of this type. On information and belief, the PII was kept unencrypted by CBC as, had proper encryption been implemented, the criminals would have exfiltrated only unintelligible

[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 June 19, 2023).

[2] "Player's Club" https://www.crystalbaycasino.com/gaming/players-club/ (last accessed June 19, 2023).

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

data. As a result, its customers' and/or employees' sensitive information was accessed and misused by unauthorized third-party hackers.

4. The potential for improper disclosure of Plaintiff's and Class Members' PII through a cyberattack was a known and foreseeable risk to CBC, and CBC was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

5. In addition, CBC and its employees failed to properly monitor the computer network and systems that housed the PII. Had CBC properly monitored its computer property, it would have discovered the intrusion sooner.

6. 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 negligent violation of their privacy rights.

7. Plaintiffs and Class Members are current and former CBC customers and/or current and former CBC employees who had their PII collected, stored, and ultimately breached by CBC.

8. Plaintiffs and Class Members have suffered injuries and damages as a result of CBC's misconduct. As a direct and proximate 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—was compromised in the Data Breach, in violation of their privacy rights. Plaintiffs and Class Members are now exposed to a present and continuing risk of identity theft and fraud for the remainder of their lifetimes and must 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 is property and has determinable market value on both legitimate and dark web marketplaces. Finally, Plaintiffs and Class Members lost the benefit of their bargain, as they would not have purchased CBC's services had they been aware that CBC would not implement reasonable and adequate safeguards to protect their PII.

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

9. Further, CBC unreasonably delayed in notifying Plaintiffs and Class Members of the Data Breach which prevented them from being able to proactively mitigate the consequences of the Data Breach.

10. 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.

11. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

12. Plaintiffs and Class Members have a continuing interest in ensuring that their information, which remains in the possession of Defendant, is and remains safe, and they should be entitled to injunctive and other equitable relief in addition to damages.

THE PARTIES

13. 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.

14. 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

[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 June 19, 2023).

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

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.

15. Plaintiff Huy Nguyen is a California citizen residing in San Leandro, California. Plaintiff Nguyen is a former customer of CBC. In or around 2018, Plaintiff Nguyen provided his sensitive PII to Defendant as a requirement to place wagers and/or bets at Defendant's casino. On or around February 24, 2023, Plaintiff Nguyen received a data breach notice from Defendant informing him that his personal information, including *inter alia*, his name, Social Security number, and driver's license number had been implicated in the data breach. As a result of the Data Breach, Plaintiff Nguyen made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; changing passwords and resecuring his own computer system; and contacting credit bureaus to place credit freezes on his account. Plaintiff Nguyen has significant time dealing with the Data Breach; valuable time Plaintiff Nguyen otherwise would have spent on other activities, including but not limited to recreation.

16. 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

17. 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). There exist members of the putative Plaintiff class that are domiciled in states diverse from Defendant, including Plaintiff Nguyen. Further, there are more than 100 putative class members, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

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

18. 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.

19. 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. Defendant's Business

20. Defendant Crystal Bay Casino is a resort and casino located in the Lake Tahoe area, on the Nevada side of the California-Nevada border. In the ordinary course of business, Defendant requires its customers and employees to provide it with their sensitive PII—including, but not limited to, their full names, Social Security numbers, and driver's license information.

21. Additionally, 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.

22. CBC stores the sensitive PII it obtains from its current and former customers and current and former employees in its internal data servers.

23. On information and belief, in the course of collecting PII from consumers and employees, including Plaintiffs, Defendant promised to provide confidentiality and adequate security for customer data through its applicable privacy policy and through other disclosures.

B. The Data Breach

24. 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 data

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

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.[4]

25. CBC's data breach was the result of a cyber-attack expressly designed and targeted to gain access to private and confidential data—including (among other things) the personal information, or PII, of Defendant's customers and clients, including Plaintiff's and Class Members' and, possibly, employees' PII—known to be stored in Defendant's internal data servers.

26. Upon information and belief, Defendant also failed to encrypt the PII stored on its server, evidenced by the fact that hackers were able to steal the PII in a readable form.

C. CBC's Unreasonably Delayed and Inadequate Notification

27. CBC owed Plaintiffs and Class Members a duty under state law to provide timely notification of the data breach.

28. Under Nev. Rev. Stat. §603A.220, CBC was required to provide such notification "in the most expedient time possible and without unreasonable delay."

29. 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 discovered that certain files had been copied from its data systems on November 27, 2022.

30. 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.

31. 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.

[4] *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 June 19, 2023).

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

32. 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.

D. CBC's Statutory Obligation to Protect Customers' & Employees' PII

33. 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."

34. 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.

35. 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.

36. Further, the Federal Trade Commission Act, 15 U.S.C. §45 prohibits CBC from engaging in "unfair or deceptive acts or practices affecting commerce."

37. 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).

38. 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.

E. Applicable Standards of Care

39. 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,

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

safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

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

41. 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.

42. 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 on how to adequately protect PII.

43. 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.

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

45. 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.

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

47. CBC owed a duty of care to Plaintiffs and the Class Members because they were the 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. CBC knew that a breach of its data systems would cause Plaintiffs and Class Members to incur damages.

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

F. The Data Breach Was A Foreseeable Risk Of Which Defendant Was On Notice

48. CBC's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the hospitality services industry preceding the date of the breach.

49. Data breaches, including those perpetrated against the hospitality services sector of the economy, have become widespread.

50. In fact, a similar data breach occurred recently involving another casino/restaurant in Nevada, which should have put CBC on notice of the threat of cyberattacks against casinos due to the sensitive PII that they maintain.[5]

51. According to Bluefin, "[t]he restaurant and hospitality industries have been hit particularly hard by data breaches, with hotel brands, restaurants and establishments targeted by hackers in 2019."[6]

52. Another report says that the "companies in the food and beverage industry are the most at risk from cybercriminals."[7]

53. According to Kroll, "data-breach notifications in the food and beverage industry shot up 1,300% in 2020."[8]

54. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[9]

55. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020. [10]

---

[5] https://www.databreaches.net/nevada-restaurant-services-inc-provides-notice-of-data-privacy-event/ (last visited on June 19, 2023).
[6] https://www.bluefin.com/bluefin-news/the-rise-in-restaurant-data-breaches-and-the-need-to-devalue-consumer-data/ (last visited on June 19, 2023).
[7] https://www.industryweek.com/finance/article/21959093/food-and-beverage-industry-most-at-risk-for-cyber-attack (last visited on June 19, 2023).
[8] https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-other-industries/d/d-id/1341336 (last visited on June 19, 2023).
[9] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[10] *Id*.

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

56. Indeed, cyber-attacks, such as the one experienced by CBC, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in CBC's industry, including CBC.

G. The Value of PII

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

58. Plaintiffs and Class Members value their PII because 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 or receiving preferred loan rates.

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

60. 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."[11]

61. 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.

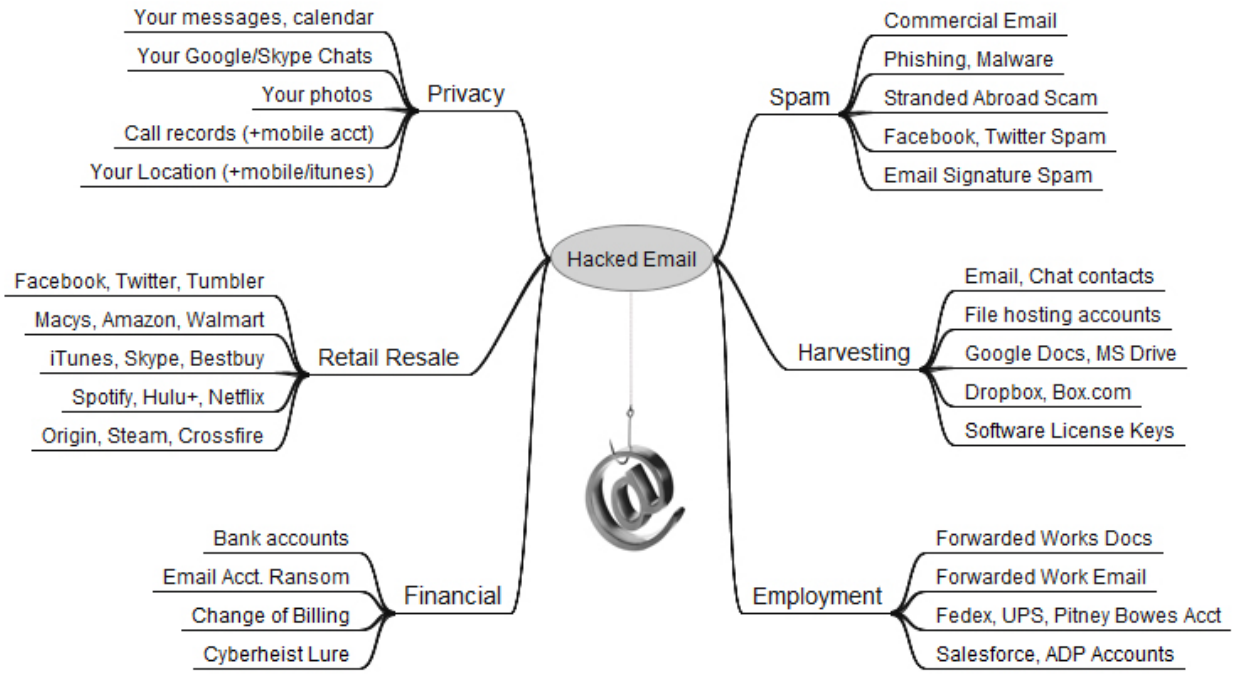
62. In addition to PII, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to

[11] *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/.

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

verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.[12]

63. 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.[13]



64. 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-

[12] *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 June 19, 2023).

[13] 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 June 19, 2023).

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

directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers."[14]

65. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information, precisely as they have done here. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

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

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

68. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[15]

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

[14] *Report on Phishing* (Oct. 2006), https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf (last accessed June 19, 2023).

[15] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a

69. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

70. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

71. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

72. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

73. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

H. Data Breach Victims Face A Heightened Risk of Identity Theft and Fraud

74. 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.

75. 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

compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

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

personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[16] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."[17]

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

76. Javelin Strategy and Research reports that losses from identity theft reached $21 billion in 2013.

77. Moreover, 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.

78. 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 June 19, 2023).

79. This is particularly the case with data breaches such as CBC, as the information compromised in this Data Breach, such as Social Security numbers, is immutable and cannot be changed. Once such information is breached, malicious actors can continue misusing the stolen information 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.[18] 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.

[16] *See Victims of Identity Theft*, U.S. Department of Justice (Dec 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

[17] *Id.*

[18] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare* (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/. (last accessed June 19, 2023).

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

J. Plaintiffs and Class Members Suffered Damages

80. 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.

81. Plaintiffs' and Class Members' PII is private and sensitive in nature and was inadequately protected by CBC who was at all times fully aware of the potential for a cyberattack targeted at acquiring the PII collected and maintained by CBC.

82. 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.

83. 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 a present, 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.

84. Plaintiffs have also lost the value of their PII. PII is a valuable commodity in both legitimate and dark web marketplaces, as evidenced by the $200 billion valuation of the data brokering industry in 2019.[19] In fact, the data marketplace is so sophisticated that consumers can

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

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

actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers. [20,21] Numerous companies purchase PII directly 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. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[22]

85. And the value of PII is further demonstrated by market-based pricing data involving the sale of stolen PII across multiple different illicit websites.

86. 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.

87. 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
- Wells Fargo bank statement: $25
- Wells Fargo bank statement with transactions: $80
- Rutgers State University student ID: $70

88. 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:

[20] https://datacoup.com/
[21] https://digi.me/what-is-digime/
[22] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

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

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

89. Plaintiffs bring 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, a Nevada Subclass (represented by Plaintiffs Fernando Mendoza and Sophia Mendoza , and a California Subclass (represented by Plaintiff Huy Nguyen). The Classes are initially defined as follows:

The Nationwide Class, initially defined as:

> All persons whose PII was compromised as a result of the cyber-attack that Defendant discovered on or about November 12, 2022 and that took place from on or about November 9, 2022 until on or about November 13, 2022, and who were sent notice of that data breach.

The Nevada Sub-Class, initially defined as:

> All persons residing in the State of Nevada whose PII was compromised as a result of the cyber-attack that Defendant discovered on or about November 12, 2022 and that took place from on or about November 9, 2022 until on or about November 13, 2022, and who were sent notice of that data breach.

The California Sub-Class, initially defined as:

> All persons residing in the State of California whose PII was compromised as a result of the cyber-attack that Defendant discovered on or about November 12, 2022 and that took place from on or about November 9, 2022 until on or about November 13, 2022, and who were sent notice of that data breach.

90. Excluded from each of the above Classes is Defendant, including any entity in

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

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 reserve the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded or otherwise modified.

91. *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.

92. *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;

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

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

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.

93. *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.

94. *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 have 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.

95. *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 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.

96. 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.

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

97. 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)

98. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 97, inclusive, of this Complaint as if set forth fully herein.

99. 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. [23] 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 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. [24] 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

///

///

[23] 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 June 19, 2023).
[24] *Id*.

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

providers have implemented reasonable security measures. [25]

100. 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.

101. 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."

102. 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 businesses are required to undertake in order to satisfy their data security obligations. [26]

103. 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

[25] 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 June 19, 2023).

[26] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-securityenforcement ((last accessed June 19, 2023).

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

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 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

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

> 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.

104. 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.

105. 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.

106. 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.

107. 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 manner.

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

109. 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.

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

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

111. 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.

112. 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.

113. 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 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.

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

115. As a direct and proximate result of Defendant's failure to adequately protect and

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

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.

116. 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)

117. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 97, inclusive, of this Complaint as if set forth fully herein.

118. Plaintiffs and Class Members provided their PII and conferred a monetary benefit upon Defendant in exchange for services and/or employment. Plaintiffs and Class Members did so under the reasonable but mistaken belief that part of their monetary payment to Defendant, or the revenue Defendant derived from the provision of labor or use of the PII, would cover the implementation of reasonable, adequate, and statutorily mandated safeguards to protect their PII. Defendant was enriched when it diverted money intended to fund adequate data security towards its own profit at the expense of Plaintiffs and Class Members.

119. Defendant's enrichment came at the expense of Plaintiffs and Class Members, who would not have used Defendant's services, would not have provided their PII, or would not have worked for Defendant, had they been aware that Defendant had not implemented reasonable, adequate and statutorily mandated safeguards to protect their PII.

120. Defendant enriched itself by saving the costs they reasonably should have

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

expended on data security measures to secure Plaintiffs' and Class Members' PII and instead directing those funds to their own profits. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

121. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

122. Defendant knew that the manner in which it maintained and transmitted PII violated industry standards and its fundamental duties to Plaintiffs and absent Class Members by neglecting well accepted security measures to ensure confidential information was not accessible to unauthorized access. Defendant had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploit, but it did not use such methods.

123. Defendant had within its exclusive knowledge, and never disclosed, that it had failed to safeguard and protect Plaintiffs and absent Class Members' PII. This information was not available to Plaintiffs, absent Class Members, or the public at large.

124. Defendant also knew that Plaintiffs and Class Members expected security against known risks and that they were required to adhere to state and federal standards for the protection of confidential personally identifying, financial, and other personal information.

125. 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.

126. Plaintiff and Class Members have no adequate remedy at law.

127. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class

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

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 Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

128. Plaintiffs repeat and incorporate by reference each and every allegation contained in paragraphs 1 through 97 inclusive of this Complaint as if set forth fully herein.

129. Defendant solicited and invited Plaintiffs and Class members to provide their PII to Defendant as a requirement of using its services, to become a member of the Player's Club, or to be eligible for employment with Defendant. Plaintiffs and Class Members accepted those offers by providing their sensitive PII to Defendant in order to obtain those benefits and services from Defendant. In doing so, Plaintiffs and Class Members entered into implied contracts with Defendant.

130. Inherent within those implied contracts was a contractual obligation that Defendants would implement reasonable and adequate data security safeguards to protect the PII that Plaintiffs and Class Members entrusted to Defendant. Upon information and belief, Defendant makes representations to those who provide it with their PII that it will implement reasonable and adequate data security safeguards to protect their PII at the time they provide their PII to Defendant. These representations serve both as a basis for and as an acknowledgement by Defendant of these implied contractual duties.

131. Plaintiffs and Class Members provided their PII to Defendant under the reasonable but mistaken belief that Defendants would implement reasonable and adequate data security safeguards to protect that PII. However, Defendant did not provide such reasonable and adequate data security. Instead, Defendant allowed Plaintiffs' and Class Members' PII to be disclosed to unauthorized third-party hackers.

132. Defendant did not comply with federal statute and regulation and did not comply with industry data security standards. In doing so, Defendant materially breached their obligations under their implied contracts with Plaintiffs and Class Members.

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

133. That Defendant would implement reasonable and adequate data security to protect PII was a material prerequisite to Plaintiffs' and Class Members' provision of that PII to Defendant. Plaintiffs and Class Members value the privacy of their PII, and do not disclose their PII to entities that do not protect it from unauthorized disclosure. Plaintiffs and Class members would not have provided their PII to Defendant had they known that Defendant would not implement such reasonable and adequate data security.

134. As a result of Defendant's breach, Plaintiffs and Class Members have been damaged. 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.

135. 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.

FOURTH CAUSE OF ACTION

Breach of Fiduciary Duty

(On Behalf of Plaintiffs and the Nationwide Class)

136. Plaintiffs repeat and incorporate by reference each and every allegation contained in paragraphs 1 through 97 inclusive of this Complaint as if set forth fully herein.

137. 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.

138. 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

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

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.

139. Plaintiff and Class Members relied on the skill and expertise of Defendant to maintain the information entrusted to it as confidential. Defendant was in an exclusive position to guard against the foreseeable threat of a cyberattack and Plaintiff and Class Members had no way to verify the integrity of Defendant's data security or to influence its policies.

140. 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.

141. 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.

142. 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

FIFTH CAUSE OF ACTION
Violation of the Nevada Deceptive Trade Practices Act ("NDTPA")
Nev. Rev. Stat. Ann. §§598.0903, *et seq.*
(On behalf of Plaintiffs Fernando Mendoza and Sophia Mendoza and the Nevada Sub-Class)

143. Plaintiffs Fernando Mendoza and Sophia Mendoza ("Plaintiffs for the purposes of this Count) repeat and incorporate by reference each and every allegation contained in paragraphs 1 through 97 inclusive of this Complaint as if set forth fully herein.

144. Plaintiffs bring this Count on their own behalf and that of the Nevada Sub-Class (the "Class" for the purposes of this Count).

145. 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.

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

147. 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.

148. 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.

149. Defendant's violations were material to consumers, such as Plaintiffs and Class Members. Had Plaintiffs and Class Members known that Defendant would not implement

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

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.

150. 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.

SIXTH CAUSE OF ACTION
Violation of the California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On behalf of Plaintiff Huy Nguyen and the California Sub-Class)

151. Plaintiff Huy Nguyen ("Plaintiff" for the purposes of this Count) repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 97 inclusive of this Complaint as if set forth fully herein.

152. Plaintiff brings this Count on his own behalf and that of the California Sub-Class (the "Class" for the purposes of this Count).

153. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

154. Defendant stored the PII of Plaintiff and Class Members in its computer systems.

155. Defendant knew or should have known that it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff's and Class Members' PII secure and prevented the loss or misuse of that PII.

156. Defendant did not disclose at any time that Plaintiff's and Class Members' PII was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only one in possession of that material information, which Defendant had a duty to disclose.

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

157. Defendant's actions and inactions violated the "unlawful" prong of the UCL. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of their computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII.

158. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, by failing to ensure its affiliates with which it directly or indirectly shared the PII did the same, and by failing to timely notify Plaintiff and Class Members of the Data Breach.

159. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiff and Class Members of the Data Breach.

160. Defendant's actions and inactions further violated the "unfair" prong of the UCL.

161. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and failure to disclose inadequacies of Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and Class Members, directly causing the harms alleged below.

162. Defendant engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

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

163. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Class Members' PII to third parties without their consent, diminution in value of their PII.

164. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiffs and Class Members outweighed their utility, if any. Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous.

165. The harms suffered by Plaintiffs and Class Members continues, as Plaintiff's and Class Members' PII remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent.

166. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g.*, In re LabMD, Inc., FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

167. Plaintiff and Class Members suffered injury in fact and lost money or property as a result of Defendant's violations of the UCL. Plaintiffs and the California Class suffered from entering into transactions with Defendant that should have included adequate data security for their PII, by experiencing a diminution of value in their Private Information as a result if its theft by cybercriminals, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their PII, the right to control that information, and additional losses as described above.

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

168. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all of the Class Members, respectfully request that the Court enters 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: June 28, 2023

Respectfully Submitted,

/s/ *Thiago M. Coelho*
Thiago M. Coelho
pro hac vice
WILSHIRE LAW FIRM, PLC

/s/ *David K. Lietz*
David K. Lietz
pro hac vice
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

Attorneys for Plaintiffs and Proposed Class

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