David Hilton Wise, Esq.
Nevada Bar No. 11014
WISE LAW FIRM, PLC
421 Court Street
Reno, Nevada, 89501
(775) 329-1766
(703) 934-6377
dwise@wiselaw.pro

M. Anderson Berry, Esq. (*pro hac vice*)
Gregory Haroutunian, Esq. (*pro hac vice*)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Attorneys for Plaintiffs and the Classes

[Additional counsel on signature page.]

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

IN RE: CASINO BREACH LITIGATION.	Case No. 2:23-cv-00276-CDS-DJA
This Document Relates to: All Actions	**CONSOLIDATED CLASS ACTION COMPLAINT**

Plaintiffs William Houghton, Andrew Figura, Michael Oldham, and Kristin Andrew ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant Rancho Mesquite Casino, Inc. dba Eureka Casino Hotel ("Eureka" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Classes, as defined below, from Defendant. Plaintiffs make the following

allegations upon information and belief, except as to their own actions, the investigation of his counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This is a data breach class action brought on behalf of consumers whose sensitive personal information was stolen by cybercriminals in a massive cyber-attack at Eureka starting on or around November 9, 2022, and lasting through on or around November 13, 2022 (the "Data Breach"). The Data Breach reportedly involved at least 229,299 individuals, a group of victims comprised of customers and, possibly, employees of Eureka.

2. Information stolen in the Data Breach included individuals' sensitive information, including at least full name, Social Security number and driver's license number. Additional sensitive data may be involved, including financial account numbers or debit/credit card numbers (in combination with security code, password, or PIN from the account) (collectively, the "Private Information" or "PII"). Plaintiffs and Class Members face an ongoing and lifetime risk of identity theft, which is heightened by the exposure of their Social Security numbers.

3. As a result of the Data Breach, Plaintiffs and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, loss of the benefit of their contractual bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

4. Plaintiffs' and Class Members' sensitive personal information—which was entrusted to Defendant, their officials and agents—was compromised, unlawfully accessed, and stolen due to the Data Breach.

5. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members

that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks of this type.

7. Upon information and belief, the mechanism of the cyber-attack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known and foreseeable risk to Defendant, and Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant adequately monitored its systems, it would have discovered the intrusion sooner.

9. Because of the Data Breach, Plaintiffs and Class Members suffered injury and damages in the form of theft and misuse of their Private Information.

10. In addition, Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Cyber-attack, data thieves can commit a variety of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. As a further result of the Data Breach, Plaintiffs and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiffs and Class Members have and may also incur out of pocket costs for, for example, purchasing credit monitoring and identity theft protection services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer damages and economic losses in the form of: the loss of time needed to: take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam messages and e-mails received as a result of the Data Breach. Plaintiffs and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own Private Information such that they are entitled to damages for unauthorized access to and misuse of their Private Information from Defendant. Further, Plaintiffs and Class Members presently and will continue to suffer from damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

15. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Data Breach.

16. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring and identity restoration services funded by Defendant to protect Plaintiffs and members of the Class for their respective lifetimes.

17. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct.

PARTIES

18. Plaintiff William Houghton is a resident and citizen of California. Plaintiff Houghton is acting on his own behalf and on behalf of others similarly situated. Eureka obtained and continues to maintain Plaintiff Houghton's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Houghton would not have entrusted his Private Information to Eureka had he known that Eureka would fail to maintain adequate data security. Plaintiff Houghton's Private Information was compromised and disclosed as a result of the Data Breach.

19. Plaintiff Micheal Oldham is a resident and citizen of Colorado. Plaintiff Oldham is acting on his own behalf and on behalf of others similarly situated. Eureka obtained and continues to maintain Plaintiff Oldham's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Oldham would not have entrusted his Private Information to Eureka had he known that Eureka would fail to maintain adequate data security. Plaintiff Oldham's Private Information was compromised and disclosed as a result of the Data Breach.

20. Plaintiff Kristen Andrew is a resident and citizen of Oregon. Plaintiff Andrew is acting on her own behalf and on behalf of others similarly situated. Eureka obtained and continues to maintain Plaintiff Andrew's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Andrew would not have entrusted her Private Information to Eureka had she known that Eureka would fail to maintain adequate data security. Plaintiff Andrew's Private Information was compromised and disclosed as a result of the Data Breach.

21. Plaintiff Andrew Figura is a resident and citizen of Nevada. Plaintiff Figura is acting on his own behalf and on behalf of others similarly situated. Eureka obtained and continues to maintain Plaintiff Figura's Private Information and has a legal duty and obligation to protect that Private

Information from unauthorized access and disclosure. Plaintiff Figura would not have entrusted his Private Information to Eureka had he known that Eureka would fail to maintain adequate data security. Plaintiff Figura's Private Information was compromised and disclosed as a result of the Data Breach.

22. Defendant Eureka is a Nevada corporation with its principal place of business at 275 Mesa Boulevard, Mesquite, Nevada, 89027.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and, upon information and belief, Plaintiffs Andrew, Houghton, and Oldham and some members of the proposed Classes are citizens of states different from Defendant.

24. This Court has jurisdiction over Defendant through its business operations in this District, the specific nature of which occurs in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, and because Plaintiff Figura resides in this judicial district.

FACTUAL ALLEGATIONS

Defendant's Business

26. Defendant owns and operates hotels and casinos in Mesquite, Nevada, Las Vegas, Nevada, and Seabrook, New Hampshire.

27. Defendant's locations offer food and beverage choices with a heavy focus on gambling.

///

///

28. In the ordinary course of doing business with Defendant, customers and employees are required to provide Defendant with sensitive, personal and private information such as, including but not limited to, the following information:

- Names
- Dates of birth
- Social Security numbers
- Driver's license numbers
- State ID numbers
- Passport numbers
- Gender information
- Financial account and/or routing numbers
- Treatment information
- Biometric data
- Taxpayer identification number
- Credit card numbers and/or expiration dates

29. As a condition of transacting with Defendant, Plaintiffs were required to disclose some or all of the Private Information listed above.[1]

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

///

[1] Eureka Casino Resort, *Privacy Policy*, https://www.eurekamesquite.com/privacypolicy (last accessed on June 6, 2023).

The Cyber-Attack and Data Breach

31. In November 2022, Eureka experienced a cybersecurity incident where some of its systems were "encrypted by an unauthorized actor."[2]

32. Beginning on or about November 9, 2022, through on or about November 13, 2022, cybercriminals gained unauthorized access to Defendant's computer systems and networks and acquired copies of Private Information held on Defendant's systems.

33. Defendant only became aware of the unauthorized access when the cyberthieves encrypted Defendant's computer systems as part of a ransomware attack.

34. A subsequent investigation showed the hacker gained access to consumers' (and possibly employees') Private Information, which included, at least, names, Social Security numbers and driver's license numbers.[3] Defendant admits that it "identified certain data that the unauthorized actor accessed during the incident."[4]

35. The cyber-attack was 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 Plaintiffs and Class Members, and possibly employees. Evidence of this specific targeting of Private Information is the fact that, according to Defendant's own forensic investigation, an "unauthorized actor was able to copy" the Private Information.

36. Defendant notified 1,737 of the impacted individuals on or about December 9, 2022, then an additional 229,299 individuals over two months later on or about February 16, 2023.[5]

///

[2] Office of the Maine Attorney General, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/35af8dca-9af6-4a5d-aa9b-d7013c99d9d6.shtml (last accessed on June 6, 2023).
[3] *Id.*
[4] *Id.*
[5] Plaintiffs' Notice of Data Breach letters are dated February 16, 2023.

37. As a result of Defendant's delay in providing notice, the risk of harm to Plaintiffs and Class Members has increased. Consumer Reports has noted: "One thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports…. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves."[6]

38. Defendant also failed to encrypt the PII stored on its computer systems, evidenced by the fact that hackers were able to steal the Private Information in a readable form.

39. Defendant acknowledges its cybersecurity and data protection was inadequate because it admits that, "[u]pon discovering the incident, we immediately took steps to secure our system..."[7]

40. Defendant also acknowledges that Plaintiffs and Class Members face a substantial and present risk of identity theft because it is actively encouraging them to "remain vigilant by reviewing your credit reports and account statements for any unauthorized activity."[8]

41. Based on the Notice of Data Breach letter they received, which informed Plaintiffs that their Private Information was removed from Defendant's network and computer systems, Plaintiffs believe their Private Information was stolen from Defendant's networks (and subsequently sold) as a result of the Data Breach.

42. Further, the removal of the Private Information from Defendant's systems demonstrates that this cyber-attack was targeted and that Plaintiffs' and Class Members' Private Information will be used for nefarious purposes.

///

[6] The Data Breach Next Door, Consumer Reports, Jan. 31, 2019, available at: https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last visited June 6, 2023).
[7] Office of the Maine Attorney General, Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/35af8dca-9af6-4a5d-aa9b-d7013c99d9d6.shtml (last visited on June 6, 2023).
[8] *Id.*

43. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

44. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

45. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the restaurant industry preceding the date of the breach.

46. Data breaches, including those perpetrated against the restaurant services sector of the economy, have become widespread. In fact, a similar data breach occurred recently involving another casino/restaurant in Nevada, where the defendant is facing a similar class action lawsuit in this Court.[9]

47. Defendant knew or should have known that these attacks were common and foreseeable. In 2022, there were 1,802 data breaches, nearly eclipsing 2021's record wherein 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[10] 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.[11] In 2019, 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[12]

---

[9] https://www.databreaches.net/nevada-restaurant-services-inc-provides-notice-of-data-privacy-event/ (last visited on June 6, 2023).

[10] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6 (last visited June 6, 2023).

[11] See *Data Breaches Hit Lots More People in 2022* (Jan. 25, 2023) https://www.cnet.com/tech/services-and-software/data-breaches-hit-lots-more-people-in-2022/ (last visited June 6, 2023).

[12] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited on June 6, 2023).

48. 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."[13]

49. Another report says that the "companies in the food and beverage industry are the most at risk from cybercriminals."[14]

50. According to Kroll, "data-breach notifications in the food and beverage industry shot up 1,300% in 2020."[15]

51. Indeed, cyber-attacks, such as the one experienced by Defendant, 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 Defendant's industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

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

53. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's

[13] https://www.bluefin.com/bluefin-news/the-rise-in-restaurant-data-breaches-and-the-need-to-devalue-consumer-data/ (last visited on June 6, 2023).

[14] https://www.industryweek.com/finance/article/21959093/food-and-beverage-industry-most-at-risk-for-cyber-attack (last visited on June 6, 2023).

[15] https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-other-industries/d/d-id/1341336 (last visited on June 6, 2023).

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

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

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

56. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

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

Defendant Failed to Comply with Industry Standards

58. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

59. Best cybersecurity practices that are standard in Defendant's industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web

browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

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

61. These foregoing frameworks are existing and applicable industry standards in Defendant's industry. Defendant knew it was a target for hackers. Despite understanding the risks and consequences of inadequate data security, Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

Defendant's Breach

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

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

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, encryptions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;

i. Failing to properly train and supervise employees in the proper handling of inbound emails.

63. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

64. Accordingly, as outlined below, Plaintiffs and Class Members now face a substantial, increased, and present and continuing risk of fraud and identity theft.

65. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

66. Defendant was well aware that the Private Information it collects is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the operators who perpetrated this cyber-attack.

///

///

///

67. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[16]

68. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

69. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

70. For example, armed with just a name and date of birth, a data thief can use 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.

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

72. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity),

[16] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited on June 6, 2023) ("GAO Report").

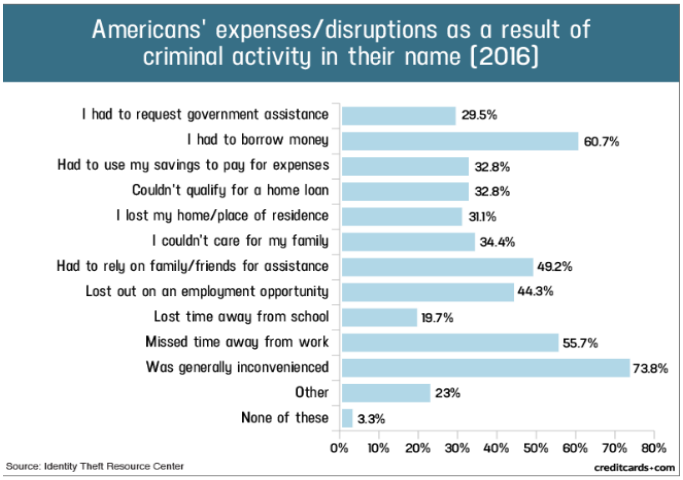
reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[17]

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

74. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

75. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

76. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[18]



[17] *See* https://www.identitytheft.gov/Steps (last visited on June 6, 2023).

[18] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020), available at: https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on June 6, 2023).

77. What's more, theft of Private Information is also gravely serious. PII is a valuable property right.[19]

78. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

79. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

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

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

See GAO Report, at p. 29.

81. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

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

---

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

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

84. Sensitive Private Information can sell for as much as $363 according to the Infosec Institute.

85. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

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

87. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.

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

89. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.

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

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

92. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[20]

93. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[21]

94. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which goes for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[22]

95. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.

---

[20] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited on June 6, 2023).

[21] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, available at: http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited on June 6, 2023).

[22] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited on June 6, 2023).

> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

96. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[23] However, this is not the case. As cybersecurity experts point out:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[24]

97. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[25]

98. At all relevant times, Defendant knew or reasonably should have known these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached and strengthened their data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiffs' and Class Members' Damages

99. To date, Defendant has done absolutely nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the cyber-attack and data breach, including, but not limited to, the costs and loss of time they incurred because of the cyber-attack. The complimentary credit monitoring service offered by Defendant is wholly inadequate as the services are only offered for

---

[23] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited on June 6, 2023).

[24] *Id.*

[25] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited on June 6, 2023).

12 months and it places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

100. Moreover, Defendant entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

101. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

Plaintiff Houghton's Experience

102. Plaintiff Houghton was required to provide his Private Information to Eureka in connection with his being a customer of Eureka beginning in or around 2011 and continuing through the present. Eureka required Plaintiff Houghton to supply it with his name, Social Security number, and other Private Information for payment and for membership in its players club. The last time he visited the casino from California was in or around 2019.

103. In or around February 2023, Plaintiff Houghton received notice from Eureka that his Private Information had been improperly accessed during a "cybersecurity incident" in November 2022. Eureka notified Plaintiff Houghton and Class members that it "identified certain data that the unauthorized actor accessed during the incident," and that the data included Plaintiff Houghton's "name, Social Security number, driver's license number or state-issued identification number." There is no indication from Defendant that the PII was encrypted or redacted in any way.

104. As a result of the Data Breach, Plaintiff Houghton 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; researching the credit monitoring and identity theft protection services offered by Eureka; and checking his credit monitoring service. Plaintiff Houghton has spent at least five hours dealing with the Data Breach; valuable time Plaintiff Houghton otherwise would have

spent on other activities, including but not limited to recreation. Plaintiff Houghton and Class Members will need identity theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the PII at issue, which includes Social Security and driver's license numbers.

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

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

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

Plaintiff Oldham's Experience

108. Plaintiff Oldham was required to provide his Private Information to Eureka in connection with his being a customer of Eureka beginning no later than 2008. Eureka required Plaintiff Oldham to supply it with his name, Social Security number, and other Private Information for payment and for membership it its players club.

109. In or around February 2023, Plaintiff Oldham received notice from Eureka that his Private Information had been improperly accessed during a "cybersecurity incident" in November 2022. Eureka notified Plaintiff Oldham and Class members that it "identified certain data that the unauthorized actor accessed during the incident," and that the data included Plaintiff Oldham's "name, Social Security number, driver's license number or state-issued identification number." There is no indication from Defendant that the PII was encrypted or redacted in any way.

110. As a result of the Data Breach, Plaintiff Oldham 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; pulling a credit report on his account; and placing a fraud alert with a credit bureau. Plaintiff Oldham has significant time dealing with the Data Breach; valuable time Plaintiff Oldham otherwise would have spent on other activities, including but not limited to recreation. Plaintiff Oldham and Class Members will need identity theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the PII at issue, which includes Social Security and driver's license numbers.

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

112. Plaintiff Oldham suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Eureka obtained from Plaintiff Oldham; (b) violation of

his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

113. As a result of the Data Breach, Plaintiff Oldham anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Oldham will continue to be at substantial and immediate risk of identity theft and fraud for years to come.

Plaintiff Andrew's Experience

114. Plaintiff Andrew was required to provide her Private Information in connection with her being a customer of Eureka over the past several years. Eureka required Plaintiff Andrew to supply it with her name, Social Security number, and other Private Information for payment and for membership in its players club.

115. In or around February 2023, Plaintiff Andrew received notice from Eureka that her Private Information had been improperly accessed during a "cybersecurity incident" in November 2022. Eureka notified Plaintiff Andrew and Class Members that it "identified certain data the unauthorized actor accessed during the incident," and the data included Plaintiff Andrew's "name and driver's license or state-issued identification number." There is no indication from Defendant that Private Information was encrypted or redacted in any way.

116. As a result of the Data Breach, Plaintiff Andrew 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; and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; Plaintiff Andrew has spent significant time dealing with the Data Breach; valuable time Plaintiff Andrew otherwise would have spent on other activities, including but not limited to recreation. Plaintiff Andrew and Class Members will need identity

theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the PII at issue, which includes driver's license numbers.

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

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

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

Plaintiff Figura's Experience

120. Plaintiff Figura was required to provide his Private Information to Eureka in connection with his being a customer of Eureka beginning no later than 2020. Eureka required Plaintiff Figura to supply it with his name and other Private Information as a condition of using Defendant's services and facilities.

121. In or around February 2023, Plaintiff Figura received notice from Eureka that his Private Information had been improperly accessed during a "cybersecurity incident" in November 2022. Eureka notified Plaintiff Figura and Class Members that it "identified certain data the unauthorized actor accessed

during the incident," and the data included Plaintiff Figura's "name and driver's license number or state-issued identification number." There is no indication from Defendant that Private Information was encrypted or redacted in any way.

122. As result of the Data Breach, Plaintiff Figura 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; and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; Plaintiff Figura has significant time dealing with the Data Breach; valuable time Plaintiff Figura otherwise would have spent on other activities, including but not limited to recreation. Plaintiff Figura and Class Members will need identity theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the PII at issue, which includes driver's license numbers.

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

124. As a result of the Data Breach, Plaintiff Figura anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Figura will continue to be at substantial and immediate risk of identity theft and fraud for years to come.

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

126. Plaintiffs and Class Members face an ongoing and substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal actions based on their Private Information as potential fraudsters could use that information to target such schemes more effectively.

127. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the cyber-attack.

128. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the cyber-attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

129. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages, in that they overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

130. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial and medical accounts and records for misuse.

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

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

132. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

133. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

134. Plaintiffs and Class Members were also injured and damaged by the delayed notice of this data breach, as it exacerbated the substantial and present risk of harm by leaving Plaintiffs and Class Members without the knowledge that would have enabled them to take proactive steps to protect themselves.

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

CLASS ACTION ALLEGATIONS

136. Plaintiffs incorporate by reference all other paragraphs of this Consolidated Complaint as if fully set forth herein.

137. Plaintiffs bring this action individually and on behalf of all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5).

138. Plaintiffs propose the following Class definitions, subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiffs bring this action and seeks certification of the following Classes:

> National Class: All persons whose PII was compromised as a result of the cyber-attack that Eureka 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 the Data Breach (the "Nationwide Class").
>
> California Class: All residents of California whose PII was compromised as a result of the cyber-attack that Eureka 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 the Data Breach (the "California Subclass") (collectively, with the Nationwide Class, "the Classes").

Excluded from the Classes are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

139. Plaintiffs reserve the right to amend the definitions of the Classes or add a Class if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

140. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

141. Numerosity. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Classes consist of more than 229,000 of Defendant's customers and employees whose data was compromised in the cyber-attack and Data Breach.

142. Commonality. 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 unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the cyber-attack complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the cyber-attack were consistent with industry standards;

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

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the cyber-attack;

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

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

j. Whether Defendant owed a duty to provide Plaintiffs and Class Members notice of this data breach, and whether Defendant breached that duty;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to an invasion of privacy;

m. Whether Defendant's actions violated federal law; and

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

143. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the cyber-attack.

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

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

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

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

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

148. Plaintiffs and the Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 147.

149. Defendant required Plaintiffs and Class Members to submit non-public personal information in order to obtain services, products and/or otherwise transact with Defendant.

150. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Plaintiffs' and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a

reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

151. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

152. Defendant's duty of care to use reasonable security measures arose Defendant were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach.

153. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

154. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;

e. Failing to detect in a timely manner that Plaintiffs' and Class Members' Private Information had been compromised;

f. Failing to timely notify Plaintiffs and Class Members about the cyber-attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

155. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

156. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would result in one or more types of injuries to Plaintiffs and Class Members.

157. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the cyber-attack and data breach.

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

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

159. Plaintiffs and the Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 147.

///

160. Through their course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

161. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services and/or products, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

162. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

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

164. Plaintiffs and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

165. The protection of Plaintiffs' and Class Members' Private Information was a material aspect of the implied contracts between Defendant and its customers, including Plaintiffs and Class Members.

166. On information and belief, the implied contracts—contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's applicable privacy policy.

167. Defendant's express representations, including, but not limited to, the express representations found in its applicable privacy policy, memorializes and embodies the implied contractual

obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

168. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

169. A meeting of the minds occurred, as Plaintiffs and Class Members agreed to and did provide their Private Information to Defendant and paid for the services and/or products Defendant furnished in exchange for, amongst other things, the protection of their Private Information.

170. Plaintiffs and Class Members performed their obligations under the contract when they paid for their services and/or products and provided their valuable Private Information.

171. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

172. Defendant materially breached the terms of the implied contracts. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by its notifications of the cyber-attack to Plaintiffs and thousands of Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and the Class Members' Private Information, as set forth above.

173. The cyber-attack and Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

174. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received

services and/or products that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the services and/or products with data security protection they paid for and the services and/or products they received.

175. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased services and/or products from Defendant.

176. As a direct and proximate result of the cyber-attack/Data Breach, Plaintiffs and Class Members have been harmed and have presently suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

177. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the cyber-attack/data breach.

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

COUNT III
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and All Class Members)

179. Plaintiffs and the Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 147.

///

180. Pursuant to Section 5 of the FTCA, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

181. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

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

183. Defendant breached its duties to Plaintiffs and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

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

185. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

186. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

187. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and All Class Members)

188. Plaintiffs and the Classes restate and reallege paragraphs 1 through 147 above as if fully set forth herein and pleads this count in the alternative to the breach of contract count (Count II) above.

189. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

190. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

191. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the cyber-attack, Defendant instead calculated to increase their 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 their own profits over the requisite security.

192. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

193. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

194. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

195. Plaintiffs and Class Members have no adequate remedy at law.

196. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

197. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

198. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

COUNT V
CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiff Houghton and the California Subclass)

199. Plaintiff Houghton and the California Subclass reallege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 147.

///

200. 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*.

201. Defendant stored the PII of Plaintiff Houghton and California Subclass Members in its computer systems.

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

203. Defendant did not disclose at any time that Plaintiff Houghton's and California Subclass 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.

Unlawful Business Practices

204. As noted above, Defendant violated Section 5(a) of the FTCA (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 Houghton's and California Subclass Members' PII.

205. Defendant also violated Section 5(a) of the FTCA 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 Houghton's and California Subclass Members of the Data Breach.

206. If Defendant had complied with these legal requirements, Plaintiff Houghton and California Subclass Members would not have suffered the damages related to the Data Breach, and

consequently from Defendant's failure to timely notify Plaintiff Houghton and California Subclass Members of the Data Breach.

207. Defendant's acts and omissions as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the FTCA.

208. Plaintiff Houghton and California Subclass Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiff Houghton's and California Subclass Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff Houghton and California Subclass Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Unfair Business Practices

209. 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 outweighs 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 Houghton and California Subclass Members, directly causing the harms alleged below.

210. 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.

211. 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 California Subclass Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff Houghton's and California Subclass Members' PII to third parties without their consent, diminution in value of their PII, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiff Houghton's and California Subclass Members' PII remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. 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).

212. Plaintiff Houghton and California Subclass Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. Plaintiff Houghton and California Subclass Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff Houghton and California Subclass Members have also suffered consequential out of pocket losses for procuring

credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

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

COUNT VI
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiff Houghton and the California Subclass)

214. Plaintiff Houghton and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 147.

215. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."

216. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

217. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party

implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

218. Section 1798.150(a)(1) of the CCPA provides:

> Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

219. Plaintiff Houghton and the California Subclass Members are "consumer[s]" as defined by Cal. Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

220. Defendant is a "business" as defined by Cal. Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

221. The Private Information taken in the Data Breach is personal information as defined by Cal. Civ. Code § 1798.81.5(d)(1)(A) because it contains Plaintiff Houghton's and the California Subclass Members' unencrypted and unredacted names and Social Security and/or driver's license and/or state-issued identification numbers.

222. Plaintiff Houghton and the California Subclass's Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their Private Information, including name and Social Security and/or driver's license and/or state-issued identification number were wrongfully taken, accessed, and viewed by unauthorized third parties.

223. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff Houghton's and the California Subclass Members' Private Information. Defendant failed to implement reasonable security procedures to prevent an attack on their server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff Houghton's and California Subclass Members' PII as a result of this attack.

224. In accordance with Cal. Civ. Code § 1798.150(b), Plaintiff Houghton provided Defendant with written notice of its alleged violations of Cal. Civ. Code § 1798.150(a). Plaintiff Houghton mailed notice by certified mail, return receipt requested, on February 22, 2023. *See* Exhibit A. Defendant timely responded to Plaintiff Houghton on March 22, 2023. *See* Exhibit B.

225. Defendant, however, did not actually cure the noticed violations. Defendant asserted, without evidence or proof, that it "cured" the above failures to implement reasonable security procedures to prevent unauthorized access of Plaintiff Houghton's and California Subclass members' PII by "[taking] measures to contain the incident, notify[ng] law enforcement, and be[ginning] an investigation." *Id.* Part of the measures Defendant took allegedly include "steps to block the unauthorized access" and "monitor[ing] for any further suspicious activity." *Id.* These post-attack actions that Defendant allegedly

took did not retroactively cure the unauthorized access, as they provide no assurance that Plaintiff Houghton's and California Subclass members' PII was not viewed by—and/or is not still in the hands of—unauthorized third parties. There was no cure at all.

226. Furthermore, none of the steps Defendant asserts in its response demonstrate an actual cure of their failure to implement reasonable security measures to protect Plaintiff Houghton's and California Subclass members' PII, as the vague steps Defendant asserts, without proof, that it has taken are not sufficient to protect Plaintiff Houghton's and California Subclass members' PII into the future.

227. Defendants' response is wholly insufficient to demonstrate any "actual cure" of their failure to implement reasonable security to protect Plaintiff Houghton's and California Subclass members' information.

228. As Defendant has not "actually cured" the violation, Plaintiff Houghton and the California Subclass seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

COUNT VII
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT ("CCRA")
Cal. Civ. Code §§ 1798.80, *et seq*.
(On Behalf of Plaintiff Houghton and the California Subclass)

229. Plaintiff Houghton and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 147.

230. The California legislature enacted the California Customer Records Act ("CCRA") to "ensure that personal information about California residents is protected." Cal. Civ. Code § 1798.81.5.

231. The CCRA states that any business which "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b).

232. Under the CCRA, personal information includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: Social Security number, Driver's license number . . . [or] medical information."

233. The personal information compromised in the Data Breach includes information that meets this definition. The information was unencrypted and unredacted as evidenced by the fact that Defendant was required to provide notification letters under the laws of several states that require notification of unauthorized access to unencrypted and unredacted information.

234. Defendant failed to maintain reasonable data security procedures appropriate to the nature of the personal information. Accordingly, Defendant violated Cal. Civ. Code § 1798.81.5(b).

235. Plaintiff Houghton and the California Subclass were injured by Defendant's violation of Cal. Civ. Code § 1798.81.5(b) and seek damages pursuant to Cal. Civ. Code § 1798.84(b). Plaintiff Houghton and the California Subclass were injured in the various ways alleged herein. They seek all monetary and non-monetary relief allowed by the CCRA to compensate for their various types of damages alleged herein.

236. Plaintiff Houghton and the California Subclass are also entitled to injunctive relief pursuant to Cal. Civ. Code § 1798.84(e), including substantial improvements to Defendant's data security systems.

COUNT VIII
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and All Class Members)

237. Plaintiffs and the Classes re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 147.

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

the terms of the federal and state statutes described in this Complaint. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their PII and remains at imminent risk that further compromises of their PII will occur in the future.

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

a. Defendant owes a legal duty to secure employees' and consumers' PII and to timely notify employees and consumers of a data breach under the common law, and Section 5 of the FTCA;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure employees' and consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs and Class Members harm.

240. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect employees' and consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards; and

d. implement an education and training program for appropriate employees regarding cybersecurity.

241. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach with Defendant. The risk of another such breach is real, immediate, and substantial. If another breach with Defendant occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

242. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

243. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose PII would be further compromised.

PRAYER FOR RELIEF

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

A. For an Order certifying the Classes, and appointing Plaintiffs and their Counsel to represent the Classes;

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

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

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

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

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

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

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

vi. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems

on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

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

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendants' network is compromised, hackers cannot gain access to portions of Defendant's systems;

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

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

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

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

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

/s/*M. Anderson Berry*
M. Anderson Berry, Esq. (*pro hac vice*)
Gregory Haroutunian, Esq. (*pro hac vice*)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

David Hilton Wise, Esq.
Nevada Bar No. 11014
WISE LAW FIRM, PLC
421 Court Street

Reno, Nevada, 89501
Telephone: (775) 329-1766
Facsimile: (703) 934-6377
dwise@wiselaw.pro

Gary M. Klinger, Esq. (*pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Bryan L. Bleichner, Esq. (*pro hac vice* forthcoming)
Philip Joseph Krzenski, Esq. (*pro hac vice* forthcoming)
CHESTNUT COMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Mark J. Bourass, Esq.
Jennifer A. Fornetter, Esq.
Valeria S. Gray, Esq.
THE BOURASSA LAW GROUP
2350 W. Charleston Boulevard, Suite 100
Las Vegas, NV 89102
Telephone: (702) 851-2180
Facsimile: (702) 851-2189
mbourassa@blgwins.com
jfornetti@blgwins.com
vgray@blgwins.com

Gary F. Lynch, Esq. (*pro hac vice*)
Patrick D. Donathen, Esq. (*pro hac vice*)
LYNCH CARPENTER, LLP
113 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
patrick@lcllp.com

Attorneys for Plaintiffs and the Classes