

1 Nathan R. Ring  
2 **STRANCH, JENNINGS & GARVEY, PLLC**  
3 3100 W. Charleston Boulevard, Suite 208  
4 Las Vegas, NV 89102  
5 Telephone: (725) 235-9750  
6 nring@stranchlaw.com

7 Jeff Ostrow\*  
8 **KOPELOWITZ OSTROW**  
9 **FERGUSON WEISELBERG GILBERT**  
10 One West Las Olas Blvd., Suite 500  
11 Fort Lauderdale, Florida 33301  
12 Telephone: 954-525-4100  
13 ostrow@kolawyers.com

14 J. Gerard Stranch IV\*  
15 **STRANCH, JENNINGS & GARVEY, PLLC**  
16 The Freedom Center  
17 223 Rosa L. Parks Avenue, Suite 200  
18 Nashville, TN 37203  
19 Telephone: (615) 254-8801  
20 gstranch@stranchlaw.com

21 *Counsel for Plaintiff and the Proposed Class*

22 **UNITED STATES DISTRICT COURT**  
23 **DISTRICT OF NEVADA**

24 **EMILY KIRWAN**, *individually and on*  
25 *behalf of all others similarly situated,*

26 Plaintiff,

27 v.

28 **MGM RESORTS INTERNATIONAL,**

Defendant.

**Case No.**

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff, Emily Kirwan, individually and on behalf of all similarly situated persons, alleges the following against MGM Resorts International (“MGM” or “Defendant”) based on personal

1 knowledge with respect to herself and on information and belief derived from, among other things,  
2 investigation by her counsel and review of public documents, as to all other matters:

3 **I. INTRODUCTION**

4  
5 1. Plaintiff brings this class action against Defendant for its failure to prevent a  
6 cyberattack that resulted in Plaintiff’s and other similarly situated Defendant consumers’ sensitive  
7 information, including, upon information and belief, their full names, dates of birth, addresses, email  
8 addresses, phone numbers, Social Security numbers and/or driver’s license numbers (“personally  
9 identifiable information” or “PII”).<sup>1</sup>

10  
11 2. Beginning on September 7, 2023 cyberattackers gained access to Defendant’s  
12 network by impersonating an IT admin and gaining access credentials. The cyberattackers then  
13 locked down Defendant’s network preventing resort guests from using their electronic room cards,  
14 Wi-Fi, ATM kiosks, electronic gaming devices, and other resort services.

15  
16 3. Thus far, two competing cybercriminal groups have taken credit for the attack  
17 against Defendant. First, a hacking group known as “The Scatter Spider” took credit, on or about  
18 September 11, 2021, for accessing and acquiring “six terabytes of data from the systems of multi-  
19 billion-dollar casino operators MGM Resorts International[.]”<sup>2</sup> Second, a ransomware group known  
20 as ALPHV took credit, on or about September 14, 2023, for deploying a ransomware attack against  
21 Defendant and “download[ing] any and all exfiltrated materials”, including “PII information  
22 contained in the exfiltrated data[.]” involved in the cyberattack.<sup>3</sup>

23  
24  
25 <sup>1</sup> <https://www.bleepingcomputer.com/news/security/mgm-resorts-shuts-down-it-systems-after-cyberattack/> (last accessed Sep. 20, 2023).

26 <sup>2</sup> <https://www.reuters.com/business/casino-giant-caesars-confirms-data-breach-2023-09-14/> (last  
27 accessed Sep. 20, 2023).

28 <sup>3</sup> <https://gist.githubusercontent.com/BushidoUK/20b81335c6729dc8e0b5997ca83fa35f/raw/a0697117e905f5094e7a5feae928806b2ba65b20/gistfile1.txt?ref=thetack.technology> (last accessed Sep. 21, 2023).



1           4. Defendant owns and operates casino gaming brands with resorts throughout the  
2 United States, which include dining, live entertainment, accommodations, shopping, and gaming.

3           5. The MGM Rewards loyalty program allows members to “earn rewards for your  
4 hotel stays, dining, slots, table games, and more. Then redeem your MGM Rewards Points to do it  
5 all over again, on [Defendant].”<sup>4</sup>

6           6. Upon information and belief, individuals, including Plaintiff and Class members,  
7 who were consumers of Defendant's entertainment services or sought to join the MGM Rewards  
8 loyalty program are required to entrust Defendant with sensitive, non-public PII, without which  
9 Defendant could not perform its regular business activities, in order to obtain entertainment products  
10 and/or services from Defendant. Defendant retains this information for at least many years and even  
11 after the consumer relationship has ended.

12           7. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and  
13 Class members, Defendant assumed legal and equitable duties to those individuals to protect and  
14 safeguard that information from unauthorized access and intrusion.

15           8. Defendant failed to adequately protect Plaintiff’s and Class members PII—and  
16 failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII  
17 was compromised due to Defendant’s negligent and/or careless acts and omissions and its utter  
18 failure to protect consumers’ sensitive data. Hackers targeted and obtained Plaintiff’s and Class  
19 members’ PII because of its value in exploiting and stealing the identities of Plaintiff and Class  
20 members. The present and continuing risk to victims of the Data Breach will remain for their  
21 respective lifetimes.

22           9. Plaintiff brings this action on behalf of all persons whose PII was compromised as  
23  
24  
25  
26  
27

28 <sup>4</sup> <https://www.mgmresorts.com/en/mgm-rewards.html> (last accessed Sep. 20, 2023).

1 a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class members; (ii)  
2 warn Plaintiff and Class members of Defendant's inadequate information security practices; and (iii)  
3 effectively secure hardware containing protected PII using reasonable and effective security  
4 procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence  
5 and violates federal and state statutes.

6  
7 10. Defendant disregarded the rights of Plaintiff and Class members by intentionally,  
8 willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable  
9 measures, failing to take available steps to prevent an unauthorized disclosure of data, and failing to  
10 follow applicable, required, and appropriate protocols, policies, and procedures regarding the  
11 encryption of data, even for internal use. As a result, the PII of Plaintiff and Class members was  
12 compromised through disclosure to an unknown and unauthorized third party.

13  
14 11. Plaintiff and Class members have a continuing interest in ensuring that their  
15 information is and remains safe, and they should be entitled to injunctive and other equitable relief.

16 12. Plaintiff and Class members have suffered injury as a result of Defendant's conduct.  
17 These injuries include: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII;  
18 (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences  
19 of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with  
20 attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and  
21 certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized  
22 third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject  
23 to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate  
24 measures to protect the PII.

25  
26 13. Plaintiff seeks to remedy these harms and prevent any future data compromise on  
27 behalf of herself and all similarly situated persons whose personal data was compromised and stolen  
28

1 as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security  
2 practices.

3 **II. PARTIES**

4 14. Plaintiff is, and at all times mentioned herein was, an individual citizen and resident  
5 of New Iberia, Louisiana.

6 15. Defendant is a Delaware corporation with its principal place of business located at  
7 3600 South Las Vegas Boulevard, Las Vegas, Nevada 89109.

8 **III. JURISDICTION AND VENUE**

9 16. The Court has subject matter jurisdiction over this action under the Class Action  
10 Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of  
11 interest and costs. The number of Class members is over 100, many of whom reside outside the state  
12 of Nevada and have different citizenship from Defendant, including Plaintiff. Thus, minimal  
13 diversity exists under 28 U.S.C. §1332(d)(2)(A).

14 17. This Court has jurisdiction over Defendant because it operates in this District.

15 18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because  
16 Defendant's principal place of business is located in this District, a substantial part of the events  
17 giving rise to this action occurred in this District, and Defendant has harmed Class members residing  
18 in this District.

19 **IV. FACTUAL ALLEGATIONS**

20 **A. Defendant's Business**

21 19. Defendant owns and operates casino gaming brands with resorts throughout the  
22 United States, which include dining, live entertainment, accommodations, shopping, and gaming.

23 20. As a necessary part of its regular business activities, Defendant collected and stored  
24 the PII of Plaintiff and Class members.

1 21. As a condition of receiving its products and/or services, Defendant requires that  
2 consumers and/or members of its MGM Rewards members, including Plaintiff and Class members,  
3 entrust it with highly sensitive personal information.

4 22. The information held by Defendant in its computer systems at the time of the Data  
5 Breach included the unencrypted PII of Plaintiff and Class members.

6 23. Upon information and belief, Defendant made promises and representations to its  
7 consumers, including Plaintiff and Class members, that the PII collected from them would be kept  
8 safe, confidential, that the privacy of that information would be maintained, and that Defendant  
9 would delete any sensitive information after it was no longer required to maintain it.

10 24. Indeed, Defendant’s Privacy Policy provides that: “[i]nformation maintained in  
11 electronic form that is collected by MGM Resorts International and any individual MGM Resort is  
12 stored on systems protected by industry standard security measures. These security measures are  
13 intended to protect these systems from unauthorized access.”<sup>5</sup>

14 25. Plaintiff and Class members provided their PII to Defendant with the reasonable  
15 expectation and on the mutual understanding that Defendant would comply with its obligations to  
16 keep such information confidential and secure from unauthorized access.

17 26. Plaintiff and the Class members have taken reasonable steps to maintain the  
18 confidentiality of their PII. Plaintiff and Class members relied on the sophistication of Defendant to  
19 keep their PII confidential and securely maintained, to use this information for necessary purposes  
20 only, and to make only authorized disclosures of this information. Plaintiff and Class members value  
21 the confidentiality of their PII and demand security to safeguard their PII.

22 27. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff  
23  
24  
25  
26  
27

28 <sup>5</sup> <https://www.mgmresorts.com/en/privacy-policy.html> (last accessed Sep. 20, 2023).



1 and Class members from involuntary disclosure to third parties. Defendant has a legal duty to keep  
2 consumer’s PII safe and confidential.

3 28. Defendant had obligations created by the FTC Act, contract, industry standards, and  
4 representations made to Plaintiff and Class members, to keep their PII confidential and to protect it  
5 from unauthorized access and disclosure.  
6

7 29. Defendant derived a substantial economic benefit from collecting Plaintiff’s and  
8 Class members’ PII. Without the required submission of PII, Defendant could not perform the  
9 services it provides.

10 30. By obtaining, collecting, using, and deriving a benefit from Plaintiff’s and Class  
11 members’ PII, Defendant assumed legal and equitable duties and knew or should have known that it  
12 was responsible for protecting Plaintiff’s and Class members’ PII from disclosure.  
13

14 **B. The Data Breach**

15 31. On September 11, 2023, MGM posted a message informing consumers that MGM  
16 experienced a cybersecurity issue affecting some of its systems.<sup>6</sup> According to one cybercriminal  
17 group that has taken credit for the attack, the cybercriminals gained access to Defendant’s systems  
18 by impersonating an employee to gain access credentials, a relatively simple social engineering  
19 attack.<sup>7</sup> Once the threat actors gained access to the network, the cybercriminals deployed  
20 ransomware designed to lock down Defendant’s network as leverage to force Defendant to pay a  
21 ransom.  
22

23 32. The attack lasted at least ten days, during which, MGM consumers reported being  
24

25  
26 <sup>6</sup>[https://twitter.com/MGMResortsIntl/status/1701256032369164399?ref\\_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1701256032369164399%7Ctwgr%5Ebd2523f4ae5a90adb166512a6dd1eb6556ac4bd%7Ctwcon%5Es1\\_&ref\\_url=https%3A%2F%2Fwww.reuters.com%2Ftechnology%2Fmoodys-says-breach-mgm-is-credit-negative-disruption-lingers-2023-09-13%2F](https://twitter.com/MGMResortsIntl/status/1701256032369164399?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1701256032369164399%7Ctwgr%5Ebd2523f4ae5a90adb166512a6dd1eb6556ac4bd%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.reuters.com%2Ftechnology%2Fmoodys-says-breach-mgm-is-credit-negative-disruption-lingers-2023-09-13%2F)  
27 (last accessed Sep. 20, 2023).  
28

<sup>7</sup> <https://techcrunch.com/2023/09/14/mgm-cyberattack-outage-scattered-spider/>



1 unable to use electronic room keycards, wireless internet, ATM kiosks, make electronic payments,  
2 use MGM resort services, and that electronic gaming devices like slot machines were offline.<sup>8</sup>

3 33. Worse still, the cyberattackers claim to exfiltrated at least six terabytes of data,  
4 which on information and belief include the PII of Plaintiff and Class members, from Defendant’s  
5 network.<sup>9</sup>

6 34. A ransomware attack, like that experienced by Defendant is a type of cyberattack  
7 that is frequently used to target companies due to the sensitive patient data they maintain.<sup>10</sup> In a  
8 ransomware attack the attackers use software to encrypt data on a compromised network, rendering  
9 it unusable and demanding payment to restore control over the network.<sup>11</sup>

10 35. Companies should treat ransomware attacks as any other data breach incident  
11 because ransomware attacks don’t just hold networks hostage, “ransomware groups sell stolen data  
12 in cybercriminal forums and dark web marketplaces for additional revenue.”<sup>12</sup> As cybersecurity  
13 expert Emisoft warns, “[a]n absence of evidence of exfiltration should not be construed to be  
14 evidence of its absence [...] the initial assumption should be that data may have been exfiltrated.”

15 36. An increasingly prevalent form of ransomware attack is the  
16 “encryption+exfiltration” attack in which the attacker encrypts a network and exfiltrates the data  
17  
18  
19  
20

21 \_\_\_\_\_  
22 <sup>8</sup> <https://www.wusa9.com/article/news/nation-world/mgm-resorts-computers-restored-after-10-day-shutdown/507-960b53d2-c1c7-4c29-8fe7-e10b17a5d203>

23 <sup>9</sup> <https://www.thestack.technology/mgm-okta-ransomware/>

24 <sup>10</sup> *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at  
25 <https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/>

26 <sup>11</sup> *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at  
27 <https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends>

28 <sup>12</sup> *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at  
<https://blog.emisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/>





1 contained within.<sup>13</sup> In 2020, over 50% of ransomware attackers exfiltrated data from a network  
2 before encrypting it.<sup>14</sup> Once the data is exfiltrated from a network, its confidential nature is  
3 destroyed and it should be “assume[d] it will be traded to other threat actors, sold, or held for a  
4 second/future extortion attempt.”<sup>15</sup> And even where companies pay for the return of data attackers  
5 often leak or sell the data regardless because there is no way to verify copies of the data are  
6 destroyed.<sup>16</sup>

7  
8 37. Defendant was aware that it was vulnerable to this type of attack because the IT  
9 vendor that it relied upon, Okta, had warned of “a consistent pattern of social engineering attacks  
10 against [] IT service desk personnel, in which the caller’s strategy was to convince service desk  
11 personnel to reset all Multi-factor Authentication (MFA) factors enrolled by highly privileged users.”  
12 Once Okta even published preventative tips to its consumers on how to prevent the type of  
13 impersonation attack suffered by Defendant and instructed consumers to:

- 14 • Protect sign-in flows by enforcing phishing-resistant authentication with Okta FastPass and  
15 FIDO2 WebAuthn.
- 16 • Configure Authentication Policies (Application Sign-on Policies) for access to privileged  
17 applications, including the Admin Console, to require re-authentication “at every sign-in”.
- 18 • If using self-service recovery, initiate recovery with the strongest available authenticator  
19 (currently Okta Verify or Google Authenticator), and limit recovery flows to trusted  
20 networks (by IP, ASN or geolocation).
- 21 • Review and consolidate the use of Remote Management and Monitoring (RMM) tools by  
22 help desk personnel, and block execution of all other RMM tools.
- 23
- 24
- 25

26 <sup>13</sup> 2020 Ransomware Marketplace Report, available at <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>

27 <sup>14</sup> Ransomware FAQs, available at <https://www.cisa.gov/stopransomware/ransomware-faqs>

28 <sup>15</sup> *Id.*

<sup>16</sup> *Id.*



3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102  
725-235-9750  
lasvegas@stranchlaw.com  
STRANCH, JENNINGS & GARVEY  
PLLC

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- Strengthen help desk identity verification processes using a combination of visual verification, delegated Workflows in which helpdesk personnel issue MFA challenges to verify a user’s identity, and/or Access Requests that require approval by a user’s line manager before factors are reset.
- Turn on and test New Device and Suspicious Activity end-user notifications.
- Review and limit the use of Super Administrator Roles - Implement privileged access management (PAM) for Super Administrator access, and use Custom Admin Roles for maintenance tasks and delegate the ability to perform high-risk tasks.
- All Administrative roles in Okta can be constrained to a specific group. We recommend using Custom Admin Roles to create help desk roles with the least privileges required in your organization, and to constrain these roles to groups that exclude highly privileged administrators.
- Enforce dedicated admin policies - Require admins to sign-in from managed devices and via phishing resistant MFA (Okta FastPass, FIDO2 WebAuthn). Restrict this access to trusted Network Zones and deny access from anonymizing proxies.<sup>17</sup>

38. Despite these warnings, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class members, allowing the attackers free access to the PII stored therein. Defendant failed to properly verify the credentials of the attacker and failed to have in place systems to prevent and detect the ransomware attack.

39. The attacker accessed and acquired at least 6 terabytes of information from Defendant’s files, which on information and belief, contained unencrypted PII of Plaintiff and Class members, including their Social Security numbers and other sensitive information. Plaintiff’s and Class members’ PII was accessed and stolen in the Data Breach.

---

<sup>17</sup> <https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection?ref=thetack.technology>

1 40. Plaintiff further believes her PII, and that of Class members has been or will be sold  
2 on the dark web, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this  
3 type.

4 **C. *Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII.***

5 41. Defendant collected, retained, and stored the PII of Plaintiff and Class members and  
6 derived a substantial economic benefit from that PII. But for the collection of Plaintiff's and Class  
7 members' PII, Defendant would be unable to perform its services.

8 42. By obtaining, collecting, and storing the PII of Plaintiff and Class members,  
9 Defendant assumed legal and equitable duties and knew or should have known that it was responsible  
10 for protecting the PII from disclosure.

11 43. Plaintiff and Class members have taken reasonable steps to maintain the  
12 confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained  
13 securely, to use this information for business purposes only, and to make only authorized disclosures  
14 of this information.

15 44. Defendant could have prevented this Data Breach by properly securing its network  
16 and encrypting the files and file servers containing the PII of Plaintiff and Class members.

17 45. Defendant made promises to Plaintiff and Class members to safely maintain and  
18 protect their PII, demonstrating an understanding of the importance of securing PII.

19 **E. *Defendant Knew or Should Have Known of the Risk Because Institutions in***  
20 ***Possession of PII Are Particularly Susceptable to Cyber Attacks.***

21 46. Defendant's data security obligations were particularly important given the  
22 substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store  
23 PII, like Defendant, preceding the date of the breach.

24 47. Data thieves regularly target companies like Defendant due to the highly sensitive  
25 information in their custody. Defendant knew and understood that unprotected PII is valuable and  
26



1 highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized  
2 access.

3 48. In 2021, a record 1,862 data breaches occurred, resulting in approximately  
4 293,927,708 sensitive records being exposed, a 68% increase from 2020.<sup>18</sup>

5  
6 49. In light of recent high profile data breaches at other industry leading companies,  
7 including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June  
8 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020),  
9 Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May  
10 2020), Defendant knew or should have known that the PII that they collected and maintained would  
11 be targeted by cybercriminals.

12 50. Despite the prevalence of public announcements of data breach and data security  
13 compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class  
14 members from being compromised.

15  
16 51. Moreover, Defendant was, or should have been, aware of the foreseeable risk of a  
17 cyberattack, like the one it experienced. Not only did Okta publish a warning directly warning of  
18 this type of attack but in 2022, BetMGM, LLC, which is owned and operated by Defendant,  
19 experienced a data breach in 2022.<sup>19</sup> Since then the records of over 1.5 million bet MGM consumers  
20 have been offered for sale on the dark web.<sup>20</sup>

21  
22 52. Accordingly, Defendant knew, or should have known, the importance of  
23 safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable  
24

---

25  
26 <sup>18</sup> See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (<https://notified.idtheftcenter.org/s/>), at 6.

27 <sup>19</sup> See <https://apps.web.maine.gov/online/aeviewer/ME/40/ef5d2df4-691f-4471-b476-5459bf590bae.shtml> (last accessed Sep. 20, 2023).

28 <sup>20</sup> <https://www.securityweek.com/betmgm-confirms-breach-hackers-offer-sell-data-15-million-customers/> (last accessed Sept. 21, 2023).

1 consequences if its data security systems were breached, including the significant costs imposed on  
2 Plaintiff and Class members as a result of a breach.

3 53. At all relevant times, Defendant knew, or reasonably should have known, of the  
4 importance of safeguarding the PII of Plaintiff and Class members and of the foreseeable  
5 consequences that would occur if Defendant's data security system was breached, including,  
6 specifically, the significant costs that would be imposed on Plaintiff and Class members as a result  
7 of a breach.

8  
9 54. Defendant was, or should have been, fully aware of the unique type and the  
10 significant volume of data on Defendant's server(s), amounting to, upon information and belief,  
11 potentially millions of individuals' detailed, PII, and, thus, the significant number of individuals who  
12 would be harmed by the exposure of the unencrypted data.

13  
14 55. The injuries to Plaintiff and Class members were directly and proximately caused  
15 by Defendant's failure to implement or maintain adequate data security measures for the PII of  
16 Plaintiff and Class members.

17 56. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class  
18 members are long lasting and severe. Once PII is stolen, fraudulent use of that information and  
19 damage to victims may continue for years.

20  
21 57. As a corporation in possession of consumers' PII, Defendant knew, or should have  
22 known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class members and  
23 of the foreseeable consequences if its data security systems were breached. This includes the  
24 significant costs imposed on Plaintiff and Class members as a result of a breach. Nevertheless,  
25 Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

**F. Value of Personally Identifiable Information**

58. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”<sup>21</sup> The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”<sup>22</sup>

59. The PII of individuals 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.<sup>23</sup>

60. For example, PII can be sold at a price ranging from \$40 to \$200.<sup>24</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>25</sup>

61. Moreover, Social Security numbers are among the worst kind of PII to have 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 experienced by Plaintiff and some Class members, can lead to identity theft and extensive financial fraud:

---

<sup>21</sup> 17 C.F.R. § 248.201 (2013).

<sup>22</sup> *Id.*

<sup>23</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, DIGITAL TRENDS, Oct. 16, 2019, <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Sept. 18, 2023).

<sup>24</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Sept. 18, 2023).

<sup>25</sup> *In the Dark*, VPNOVERVIEW, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Sept. 18, 2023).

3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102  
725-235-9750  
lasvegas@stranchlaw.com  
STRANCH, JENNINGS & GARVEY  
PLLC



1 A dishonest person who has your Social Security number can use it to get other personal  
2 information about you. Identity thieves can use your number and your good credit to apply  
3 for more credit in your name. Then, they use the credit cards and don't pay the bills, it  
4 damages your credit. You may not find out that someone is using your number until you're  
5 turned down for credit, or you begin to get calls from unknown creditors demanding payment  
6 for items you never bought. Someone illegally using your Social Security number and  
7 assuming your identity can cause a lot of problems.<sup>26</sup>

9 62. Driver's license numbers, which were likely compromised in the Data Breach, are  
10 incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of  
11 information."<sup>27</sup>

13 63. A driver's license can be a critical part of a fraudulent, synthetic identity – which go  
14 for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200.<sup>28</sup>

15 64. According to national credit bureau Experian:

16 A driver's license is an identity thief's paradise. With that one card, someone knows your  
17 birthdate, address, and even your height, eye color, and signature. If someone gets your  
18 driver's license number, it is also concerning because it's connected to your vehicle  
19 registration and insurance policies, as well as records on file with the Department of Motor  
20 Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's  
21 office, government agencies, and other entities. Having access to that one number can  
22

23  
24  
25 <sup>26</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at:  
<https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Oct. 17, 2022).

26 <sup>27</sup> *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr.  
27 20, 2021, available at: [https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-](https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658)  
28 [customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658](https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658) (last visited  
July 31, 2023).

<sup>28</sup> [https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-](https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658)  
from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited on Feb. 21, 2023).

1 provide an identity thief with several pieces of information they want to know about you.  
2 Next to your Social Security number, your driver's license number is one of the most  
3 important pieces of information to keep safe from thieves.  
4

5 65. According to cybersecurity specialty publication CPO Magazine, “[t]o those  
6 unfamiliar with the world of fraud, driver’s license numbers might seem like a relatively harmless  
7 piece of information to lose if it happens in isolation.”<sup>29</sup> However, this is not the case. As  
8 cybersecurity experts point out:

9 “It’s a gold mine for hackers. With a driver’s license number, bad actors can manufacture  
10 fake IDs, slotting in the number for any form that requires ID verification, or use the  
11 information to craft curated social engineering phishing attacks.”<sup>30</sup>  
12

13 66. Victims of driver’s license number theft also often suffer unemployment benefit  
14 fraud, as described in a recent New York Times article.<sup>31</sup>

15 67. Based on the foregoing, the information at issue in the Data Breach is significantly  
16 more valuable than the loss of, for example, credit card information in a retailer data breach because,  
17 there, victims can cancel or close credit and debit card accounts. The information compromised in  
18 this Data Breach is impossible to “close” and difficult, if not impossible, to change.

19 68. This data demands a much higher price on the black market. Martin Walter, senior  
20 director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally  
21

22  
23  
24  
25 <sup>29</sup> [https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-](https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/)  
26 [advises-customers-to-watch-out-for-fraudulent-unemployment-claims/](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 Feb. 21,  
27 2023).

28 <sup>30</sup> *Id.*

<sup>31</sup> *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 Sept. 21, 2023).



1 identifiable information . . . [is] worth more than 10x on the black market.”<sup>32</sup>

2 69. Among other forms of fraud, identity thieves may obtain driver’s licenses,  
3 government benefits, medical services, and housing or even give false information to police.

4 70. The fraudulent activity resulting from the Data Breach may not come to light for  
5 years. There may be a time lag between when harm occurs versus when it is discovered, and also  
6 between when PII is stolen and when it is used. According to the U.S. Government Accountability  
7 Office (“GAO”), which conducted a study regarding data breaches:

9 [L]aw enforcement officials told us that in some cases, stolen data may be held for  
10 up to a year or more before being used to commit identity theft. Further, once stolen  
11 data have been sold or posted on the Web, fraudulent use of that information may  
12 continue for years. As a result, studies that attempt to measure the harm resulting  
13 from data breaches cannot necessarily rule out all future harm.<sup>33</sup>

14 **G. Defendant Failed to Comply with FTC Guidelines.**

15 71. The Federal Trade Commission (“FTC”) has promulgated numerous guides for  
16 businesses which highlight the importance of implementing reasonable data security practices.  
17 According to the FTC, the need for data security should be factored into all business decision  
18 making. Indeed, the FTC has concluded that a company’s failure to maintain reasonable and  
19 appropriate data security for consumers’ sensitive personal information is an ‘unfair practice’ in  
20 violation of Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. *See, e.g.,*  
21 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).  
22  
23

24  
25  
26 <sup>32</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*  
27 *Numbers*, IT WORLD (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Sept. 18, 2023).

28 <sup>33</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Sept. 18, 2023).



1           72.       In October 2016, the FTC updated its publication, Protecting Personal Information:  
2 A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines  
3 note that businesses should protect the personal consumer information that they keep, properly  
4 dispose of personal information that is no longer needed, encrypt information stored on computer  
5 networks, understand their network’s vulnerabilities, and implement policies to correct any security  
6 problems. The guidelines also recommend that businesses use an intrusion detection system to  
7 expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is  
8 attempting to hack into the system, watch for large amounts of data being transmitted from the  
9 system, and have a response plan ready in the event of a breach.  
10

11           73.       The FTC further recommends that companies not maintain PII longer than is needed  
12 for authorization of a transaction, limit access to sensitive data, require complex passwords to be  
13 used on networks, use industry-tested methods for security, monitor the network for suspicious  
14 activity, and verify that third-party service providers have implemented reasonable security  
15 measures.  
16

17           74.       The FTC has brought enforcement actions against businesses for failing to  
18 adequately and reasonably protect consumer data by treating the failure to employ reasonable and  
19 appropriate measures to protect against unauthorized access to confidential consumer data as an  
20 unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the  
21 measures businesses must take to meet their data security obligations.  
22

23           75.       As evidenced by the Data Breach, Defendant failed to properly implement basic  
24 data security practices and failed to audit, monitor, or ensure the integrity of its vendor’s data security  
25 practices. Defendant’s failure to employ reasonable and appropriate measures to protect against  
26 unauthorized access to Plaintiff’s and Class members’ PII constitutes an unfair act or practice  
27 prohibited by Section 5 of the FTCA.  
28

3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102  
725-235-9750  
lasvegas@stranchlaw.com  
STRANCH, JENNINGS & GARVEY  
PLLC



1 76. Defendant was at all times fully aware of its obligation to protect the PII of its  
2 consumers yet failed to comply with such obligations. Defendant was also aware of the significant  
3 repercussions that would result from its failure to do so.

4 **H. Defendant Failed to Comply with Industry Standards.**

5  
6 77. As noted above, experts studying cybersecurity routinely identify entertainment  
7 companies as being particularly vulnerable to cyberattacks because of the value of the PII which  
8 they collect and maintain.

9 78. Some industry best practices that should be implemented by entertainment  
10 companies dealing with sensitive PII, like Defendant, include but are not limited to: educating all  
11 employees, strong password requirements, multilayer security including firewalls, anti-virus and  
12 anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which  
13 employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow  
14 some or all of these industry best practices.

15  
16 79. Other best cybersecurity practices that are standard in the entertainment industry  
17 include: installing appropriate malware detection software; monitoring and limiting network ports;  
18 protecting web browsers and email management systems; setting up network systems such as  
19 firewalls, switches, and routers; monitoring and protecting physical security systems; and training  
20 staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these  
21 cybersecurity best practices.

22  
23 80. Defendant failed to meet the minimum standards of any of the following  
24 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-  
25 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,  
26 PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet  
27 Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable  
28



1 cybersecurity readiness.

2 81. Defendant failed to comply with these accepted standards in the entertainment  
3 industry, thereby permitting the Data Breach to occur.

4 **I. Defendant Breached Its Duty to Safeguard Plaintiff's and Class members' PII.**

5 82. In addition to its obligations under federal and state laws, Defendant owed a duty to  
6 Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing,  
7 safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen,  
8 accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class  
9 members to provide reasonable security, including consistency with industry standards and  
10 requirements, and to ensure that its computer systems, networks, and protocols adequately protected  
11 the PII of Class members.  
12

13 83. Had Defendant remedied the deficiencies in its information storage and security  
14 systems, followed industry guidelines, and adopted security measures recommended by experts in  
15 the field, it could have prevented intrusion into its information storage and security systems and,  
16 ultimately, the theft of Plaintiff's and Class members' confidential PII.  
17

18 **J. Common Injuries & Damages**

19 84. As a result of Defendant's ineffective and inadequate data security practices, the  
20 Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the  
21 risk of identity theft to the Plaintiff and Class members has materialized and is present and  
22 continuing, and Plaintiff and Class members have all sustained actual injuries and damages,  
23 including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the  
24 materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price  
25 premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued  
26 risk to their PII, which remains in the possession of Defendant, and which is subject to further  
27  
28



1 breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect  
2 Plaintiff's and Class members' PII.

3 **K. The Data Breach Increases Victims' Risk of Identity Theft.**

4 85. Plaintiff and Class members are at a heightened risk of identity theft for years to  
5 come.

6 86. The unencrypted PII of Plaintiff and Class members will end up for sale on the dark  
7 web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the  
8 hands of companies that will use the detailed PII for targeted marketing without the approval of  
9 Plaintiff and Class members. Unauthorized individuals can easily access the PII of Plaintiff and Class  
10 members.

11 87. The link between a data breach and the risk of identity theft is simple and well  
12 established. Criminals acquire and steal PII to monetize the information. Criminals monetize the  
13 data by selling the stolen information on the black market to other criminals who then utilize the  
14 information to commit a variety of identity theft related crimes discussed below.

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

19 89. For example, armed with just a name and date of birth, a data thief can utilize a  
20 hacking technique referred to as "social engineering" to obtain even more information about a  
21 victim's identity, such as a person's login credentials or Social Security number. Social engineering  
22 is a form of hacking whereby a data thief uses previously acquired information to manipulate and  
23 trick individuals into disclosing additional confidential or personal information through means such  
24 as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point  
25  
26  
27  
28



1 for these additional targeted attacks on the victim.

2 90. One such example of criminals piecing together bits and pieces of compromised PII  
3 for profit is the development of “Fullz” packages.<sup>34</sup>

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

7 92. The development of “Fullz” packages means here that the stolen PII from the Data  
8 Breach can easily be used to link and identify it to Plaintiff’s and Class members’ phone numbers,  
9 email addresses, and other unregulated sources and identifiers. In other words, even if certain  
10 information such as emails, phone numbers, or credit card numbers may not be included in the PII  
11 that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it  
12 at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers)  
13 over and over.

14 93. The existence and prevalence of “Fullz” packages means that the PII stolen from  
15 the data breach can easily be linked to the unregulated data (like driver’s license numbers) of Plaintiff  
16 and the other Class members.

17  
18  
19  
20  
21  
22 <sup>34</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including, but not  
23 limited to, the name, address, credit card information, Social Security number, date of birth, and  
24 more. As a rule of thumb, the more information you have on a victim, the more money that can be  
25 made off those credentials. Fullz are usually pricier than standard credit card credentials,  
26 commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning  
27 credentials into money) in various ways, including performing bank transactions over the phone with  
28 the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated  
with credit cards that are no longer valid, can still be used for numerous purposes, including tax  
refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account  
that will accept a fraudulent money transfer from a compromised account) without the victim’s  
knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life  
Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm> (last visited Sept. 18, 2023).



1 94. Thus, even if certain information (such as driver’s license numbers) was not stolen  
2 in the data breach, criminals can still easily create a comprehensive “Fullz” package.

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

5  
6 **L. *Loss Of Time to Mitigate Risk of Identity Theft and Fraud***

7 96. As a result of the recognized risk of identity theft, when a data breach occurs, and  
8 an individual is notified by a company that their PII was compromised, as in this Data Breach, the  
9 reasonable person is expected to take steps and spend time to address the dangerous situation, learn  
10 about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud.  
11 Failure to spend time taking steps to review accounts or credit reports could expose the individual  
12 to greater financial harm—yet, the resource and asset of time has been lost.

13 97. Plaintiff and Class members have spent, and will spend additional time in the future,  
14 on a variety of prudent actions to remedy the harms they have or may experience as a result of the  
15 Data Breach, such as researching and verifying the legitimacy of the Data Breach.

16 98. These efforts are consistent with the U.S. Government Accountability Office that  
17 released a report in 2007 regarding data breaches in which it noted that victims of identity theft will  
18 face “substantial costs and time to repair the damage to their good name and credit record.”<sup>35</sup>

19 99. These efforts are also consistent with the steps the FTC recommends data breach  
20 victims take to protect their personal and financial information after a data breach, including:  
21 contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts  
22 for seven years if someone steals their identity), reviewing their credit reports, contacting companies  
23  
24  
25  
26

27 <sup>35</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data  
28 Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full  
Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).



1 to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and  
2 correcting their credit reports.<sup>36</sup>

3 100. And for those Class members who experience actual identity theft and fraud, the  
4 GAO Report notes that victims of identity theft will face “substantial costs and time to repair the  
5 damage to their good name and credit record.”<sup>37</sup>

6  
7 **M. Diminution of Value of PII**

8 101. PII is a valuable property right.<sup>38</sup> Its value is axiomatic, considering the value of Big  
9 Data in corporate America and the consequences of cyber thefts include heavy prison sentences.  
10 Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market  
11 value.

12 102. An active and robust legitimate marketplace for PII exists. In 2019, the data  
13 brokering industry was worth roughly \$200 billion.<sup>39</sup>

14 103. In fact, the data marketplace is so sophisticated that consumers can actually sell their  
15 non-public information directly to a data broker who in turn aggregates the information and provides  
16 it to marketers or app developers.<sup>40,41</sup>

17 104. Consumers who agree to provide their web browsing history to the Nielsen  
18  
19  
20  
21

22  
23 <sup>36</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last  
visited Sept. 18, 2023).

24 <sup>37</sup> See GAO Report.

25 <sup>38</sup> See, e.g., Randall 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,  
26 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).

27 <sup>39</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last visited Sept. 18,  
2023).

28 <sup>40</sup> <https://datacoup.com/> (last visited Sept. 18, 2023).

<sup>41</sup> <https://digi.me/what-is-digime/> (last visited Sept. 18, 2023).





1 Corporation can receive up to \$50.00 a year.<sup>42</sup>

2 105. Conversely, sensitive PII can sell for as much as \$363 per record on the dark web  
3 according to the Infosec Institute.<sup>43</sup>

4 106. As a result of the Data Breach, Plaintiff's and Class members' PII, which has an  
5 inherent market value in both legitimate and dark markets, has been damaged and diminished by its  
6 compromise and unauthorized release. However, this transfer of value occurred without any  
7 consideration paid to Plaintiff or Class members for their property, resulting in an economic loss.  
8 Moreover, the PII is now readily available, and the rarity of the PII has been lost, thereby causing  
9 additional loss of value.

10 107. At all relevant times, Defendant knew, or reasonably should have known, of the  
11 importance of safeguarding the PII of Plaintiff and Class members, and of the foreseeable  
12 consequences that would occur if Defendant's data security system was breached, including,  
13 specifically, the significant costs that would be imposed on Plaintiff and Class members as a result  
14 of a breach.

15 108. Defendant was, or should have been, fully aware of the unique type and the  
16 significant volume of data on Defendant's network, amounting to, upon information and belief,  
17 millions of individuals' detailed personal information, upon information and belief, and thus, the  
18 significant number of individuals who would be harmed by the exposure of the unencrypted data.

19 109. The injuries to Plaintiff and Class members were directly and proximately caused  
20 by Defendant's failure to implement or maintain adequate data security measures for the PII of  
21

22  
23  
24  
25  
26 <sup>42</sup> Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html> (last visited Sept. 18, 2023).

27 <sup>43</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),  
28 <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>  
(last visited Sept. 18, 2023).

1 Plaintiff and Class members.

2 **N. *Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary.***

3 110. Given the type of targeted attack in this case and sophisticated criminal activity, the  
4 type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability  
5 that entire batches of stolen information have been placed, or will be placed, on the black  
6 market/dark web for sale and purchase by criminals intending to utilize the Private Information for  
7 identity theft crimes —*e.g.*, opening bank accounts in the victims’ names to make purchases or to  
8 launder money; file false tax returns; take out loans or lines of credit; or file false unemployment  
9 claims.

10  
11 111. Such fraud may go undetected until debt collection calls commence months, or even  
12 years, later. An individual may not know that his or her Social Security Number was used to file for  
13 unemployment benefits until law enforcement notifies the individual’s employer of the suspected  
14 fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return  
15 is rejected.

16  
17 112. Consequently, Plaintiff and Class members are at a present and continuous risk of  
18 fraud and identity theft for many years into the future.

19  
20 113. The retail cost of credit monitoring and identity theft monitoring can cost around  
21 \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class  
22 members from the risk of identity theft that arose from Defendant’s Data Breach. This is a future  
23 cost that Plaintiff and Class members would not need to bear but for Defendant’s failure to safeguard  
24 their PII.

25 **O. *Loss of the Benefit of the Bargain***

26 114. Furthermore, Defendant’s poor data security deprived Plaintiff and Class members  
27 of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for products and/or  
28

3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102  
725-235-9750  
lasvegas@stranchlaw.com  
STRANCH, JENNINGS & GARVEY  
PLLC



1 services, Plaintiff and other reasonable consumers understood and expected that they were, in part,  
2 paying for the product and/or service and necessary data security to protect the PII, when in fact,  
3 Defendant did not provide the expected data security. Accordingly, Plaintiff and Class members  
4 received products and/or services that were of a lesser value than what they reasonably expected to  
5 receive under the bargains they struck with Defendant.

7 **P. *Plaintiff's Experience***

8 115. Plaintiff is a current MGM Rewards member.

9 116. In order to obtain an MGM Rewards membership, Plaintiff was required to provide  
10 her PII to Defendant, including her name, date of birth, contact information, and Social Security  
11 number.

12 117. Upon information and belief, at the time of the Data Breach, Defendant retained  
13 Plaintiff's PII in its system.

14 118. Plaintiff is very careful about sharing her sensitive PII. Plaintiff stores any  
15 documents containing her PII in a safe and secure location. She has never knowingly transmitted  
16 unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have  
17 entrusted her PII to Defendant had he known of Defendant's lax data security policies.

18 119. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff  
19 made reasonable efforts to mitigate the impact of the Data Breach, including changing her debit card  
20 pin number and monitoring her financial accounts for fraudulent activity. Plaintiff has spent  
21 significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent  
22 on other activities, including but not limited to work and/or recreation. This time has been lost  
23 forever and cannot be recaptured.

24 120. Plaintiff suffered actual injury from having her PII compromised as a result of the  
25 Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or  
26  
27  
28

725-235-9750  
lasvegas@stranchlaw.com  
3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102  
STRANCH, JENNINGS & GARVEY  
PLLC

1 diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate  
2 the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity  
3 costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii)  
4 the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available  
5 for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's  
6 possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake  
7 appropriate and adequate measures to protect the PII.

9 121. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has  
10 been compounded by the fact that Defendant has still not fully informed her of key details about the  
11 Data Breach's occurrence.

12 122. As a result of the Data Breach, Plaintiff anticipates spending considerable time and  
13 money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

14 123. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be  
15 at increased risk of identity theft and fraud for years to come.

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

19  
20  
21 **V. CLASS ACTION ALLEGATIONS**

22 125. Plaintiff brings this action individually and on behalf of all other persons similarly  
23 situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

24 126. Specifically, Plaintiff proposes the following class definition, subject to amendment  
25 as appropriate:

26 All individuals in the United States whose PII was disclosed in the Data Breach (the  
27 "Class").  
28

3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102  
725-235-9750  
lasvegas@stranchlaw.com  
STRANCH, JENNINGS & GARVEY  
PLLC



1  
2 127. Excluded from the Class are Defendant and its parents or subsidiaries, any entities  
3 in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives,  
4 heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is  
5 assigned as well as their judicial staff and immediate family members.  
6

7 128. Plaintiff reserves the right to modify or amend the definition of the proposed Class,  
8 as well as add subclasses, before the Court determines whether certification is appropriate.

9 129. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a),  
10 (b)(2), and (b)(3).

11 130. Numerosity. The Class members are so numerous that joinder of all members is  
12 impracticable. Upon information and belief, Plaintiff believes that the proposed Class includes  
13 potentially millions of individuals who have been damaged by Defendant's conduct as alleged  
14 herein. The precise number of Class members is unknown to Plaintiff but may be ascertained from  
15 Defendant's records.  
16

17 131. Commonality. There are questions of law and fact common to the Class which  
18 predominate over any questions affecting only individual Class members. These common questions  
19 of law and fact include, without limitation:  
20

- 21 a. Whether Defendant engaged in the conduct alleged herein;
- 22 b. Whether Defendant's conduct violated the FTCA;
- 23 c. When Defendant learned of the Data Breach;
- 24 d. Whether Defendant's response to the Data Breach was adequate;
- 25 e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiff's and Class  
26 members' PII;
- 27 f. Whether Defendant failed to implement and maintain reasonable security  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;
- g. Whether Defendant’s data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
  - h. Whether Defendant’s data security systems prior to and during the Data Breach were consistent with industry standards;
  - i. Whether Defendant owed a duty to Class members to safeguard their PII;
  - j. Whether Defendant breached its duty to Class members to safeguard their PII;
  - k. Whether hackers obtained Class members’ PII via the Data Breach;
  - l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class members;
  - m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;
  - n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
  - o. What damages Plaintiff and Class members suffered as a result of Defendant’s misconduct;
  - p. Whether Defendant’s conduct was negligent;
  - q. Whether Defendant was unjustly enriched;
  - r. Whether Plaintiff and Class members are entitled to actual and/or statutory damages;
  - s. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief; and
  - t. Whether Plaintiff and Class members are entitled to equitable relief, including

1 injunctive relief, restitution, disgorgement, and/or the establishment of a  
2 constructive trust.

3 132. Typicality. Plaintiff's claims are typical of those of other Class members because  
4 Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.  
5 Plaintiff's claims are typical of those of the other Class members because, *inter alia*, all Class  
6 members were injured through the common misconduct of Defendant. Plaintiff is advancing the  
7 same claims and legal theories on behalf of herself and all other Class members, and there are no  
8 defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class members arise from  
9 the same operative facts and are based on the same legal theories.  
10

11 133. Adequacy of Representation. Plaintiff will fairly and adequately represent and  
12 protect the interests of Class members. Plaintiff's counsel is competent and experienced in litigating  
13 class actions, including data privacy litigation of this kind.  
14

15 134. Predominance. Defendant has engaged in a common course of conduct toward  
16 Plaintiff and Class members in that all of Plaintiff's and Class members' data was stored on the same  
17 computer systems and unlawfully accessed and exfiltrated in the same way. The common issues  
18 arising from Defendant's conduct affecting Class members set out above predominate over any  
19 individualized issues. Adjudication of these common issues in a single action has important and  
20 desirable advantages of judicial economy.  
21

22 135. Superiority. A Class action is superior to other available methods for the fair and  
23 efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in  
24 the management of this class action. Class treatment of common questions of law and fact is superior  
25 to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members  
26 would likely find that the cost of litigating their individual claims is prohibitively high and would  
27 therefore have no effective remedy. The prosecution of separate actions by individual Class members  
28

1 would create a risk of inconsistent or varying adjudications with respect to individual Class  
2 members, which would establish incompatible standards of conduct for Defendant. In contrast,  
3 conducting this action as a class action presents far fewer management difficulties, conserves judicial  
4 resources and the parties' resources, and protects the rights of each Class Member.

5  
6 136. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendant has  
7 acted and/or refused to act on grounds generally applicable to the Class such that final injunctive  
8 relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

9 137. Finally, all members of the proposed Class are readily ascertainable. Defendant has  
10 access to the names and addresses and/or email addresses of Class members affected by the Data  
11 Breach.

12  
13 **COUNT I**  
14 **Negligence and Negligence *Per Se***  
15 **(On Behalf of Plaintiff and the Class)**

16 138. Plaintiff restates and realleges paragraphs 1 through 137 above as if fully set forth  
17 herein.

18 139. Defendant requires its consumers, including Plaintiff and Class members, to  
19 submit non-public PII in the ordinary course of providing its services.

20 140. Defendant gathered and stored the PII of Plaintiff and Class members as part of its  
21 business of soliciting its services to its consumers, which solicitations and services affect  
22 commerce.

23 141. Plaintiff and Class members entrusted Defendant with their PII with the  
24 understanding that Defendant would safeguard their information.

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

27 143. By assuming the responsibility to collect and store this data, and in fact doing so,  
28





1 and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable  
2 means to secure and to prevent disclosure of the information, and to safeguard the information from  
3 theft.

4  
5 144. Defendant had a duty to employ reasonable security measures under Section 5 of  
6 the FTCA, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,”  
7 including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable  
8 measures to protect confidential data.

9 145. Defendant owed a duty of care to Plaintiff and Class members to provide data  
10 security consistent with industry standards and other requirements discussed herein, and to ensure  
11 that its systems and networks, and the personnel responsible for them, adequately protected the PII.

12  
13 146. Defendant's duty of care to use reasonable security measures arose as a result of  
14 the special relationship that existed between Defendant and Plaintiff and Class members. That  
15 special relationship arose because Plaintiff and the Class entrusted Defendant with their  
16 confidential PII, a necessary part of being consumers of Defendant.

17 147. Defendant's duty to use reasonable care in protecting confidential data arose not  
18 only as a result of the statutes and regulations described above, but also because Defendant is bound  
19 by industry standards to protect confidential PII.

20  
21 148. Defendant was subject to an “independent duty,” untethered to any contract  
22 between Defendant and Plaintiff or the Class.

23 149. Defendant also had a duty to exercise appropriate clearinghouse practices to  
24 remove former consumers' PII it was no longer required to retain pursuant to regulations.

25 150. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and  
26 the Class of the Data Breach.

27  
28 151. Defendant had and continues to have a duty to adequately disclose that the PII of

1 Plaintiff and the Class within Defendant’s possession might have been compromised, how it was  
2 compromised, and precisely the types of data that were compromised and when. Such notice was  
3 necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity  
4 theft and the fraudulent use of their PII by third parties.

5  
6 152. Defendant breached its duties, pursuant to the FTCA and other applicable  
7 standards, and thus was negligent, by failing to use reasonable measures to protect Class members’  
8 PII. The specific negligent acts and omissions committed by Defendant include, but are not limited  
9 to, the following:

- 10 a. Failing to adopt, implement, and maintain adequate security measures to safeguard  
11 Class members’ PII;
- 12 b. Failing to adequately monitor the security of their networks and systems;
- 13 c. Failing to audit, monitor, or ensure the integrity of its vendor’s data security practices;
- 14 d. Allowing unauthorized access to Class members’ PII;
- 15 e. Failing to detect in a timely manner that Class members’ PII had been compromised;
- 16 f. Failing to remove former consumers’ PII it was no longer required to retain pursuant  
17 to regulations; and
- 18 g. Failing to timely and adequately notify Class members about the Data Breach’s  
19 occurrence and scope, so that they could take appropriate steps to mitigate the  
20 potential for identity theft and other damages.

21  
22  
23 153. Defendant violated Section 5 of the FTCA by failing to use reasonable measures  
24 to protect PII and not complying with applicable industry standards, as described in detail herein.  
25 Defendant’s conduct was particularly unreasonable given the nature and amount of PII it obtained  
26 and stored and the foreseeable consequences of the immense damages that would result to Plaintiff  
27 and the Class.  
28



1 154. Plaintiff and Class members were within the class of persons the FTCA was  
2 intended to protect and the type of harm that resulted from the Data Breach was the type of harm it  
3 was intended to guard against.

4 155. Defendant's violation of Section 5 of the FTCA constitutes negligence *per se*.

5 156. The FTC has pursued enforcement actions against businesses, which, as a result of  
6 their failure to employ reasonable data security measures and avoid unfair and deceptive practices,  
7 caused the same harm as that suffered by Plaintiff and the Class.  
8

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

11 158. It was foreseeable that Defendant's failure to use reasonable measures to protect  
12 Class members' PII would result in injury to Class members. Further, the breach of security was  
13 reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the  
14 entertainment industry.  
15

16 159. Defendant has full knowledge of the sensitivity of the PII and the types of harm  
17 that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

18 160. Plaintiff and the Class were the foreseeable and probable victims of any inadequate  
19 security practices and procedures. Defendant knew or should have known of the inherent risks in  
20 collecting and storing the PII of Plaintiff and the Class, the critical importance of providing  
21 adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.  
22

23 161. It was therefore foreseeable that the failure to adequately safeguard Class  
24 members' PII would result in one or more types of injuries to Class members.

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

27 163. Defendant was in a position to protect against the harm suffered by Plaintiff and  
28

1 the Class as a result of the Data Breach.

2 164. Defendant's duty extended to protecting Plaintiff and the Class from the risk of  
3 foreseeable criminal conduct of third parties, which has been recognized in situations where the  
4 actor's own conduct or misconduct exposes another to the risk or defeats protections put in place  
5 to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second)  
6 of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific  
7 duty to reasonably safeguard personal information.  
8

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

11 166. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and  
12 the Class, the PII of Plaintiff and the Class would not have been compromised.  
13

14 167. There is a close causal connection between Defendant's failure to implement  
15 security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent  
16 harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed  
17 as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII  
18 by adopting, implementing, and maintaining appropriate security measures.  
19

20 168. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class  
21 have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft  
22 of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with  
23 attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain;  
24 (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the  
25 Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains  
26 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains  
27 backed up in Defendant's possession and is subject to further unauthorized disclosures so long as  
28

3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102  
725-235-9750  
lasvegas@stranchlaw.com  
STRANCH, JENNINGS & GARVEY  
PLLC



1 Defendant fails to undertake appropriate and adequate measures to protect the PII.

2 169. As a direct and proximate result of Defendant’s negligence, Plaintiff and the Class  
3 have suffered and will continue to suffer other forms of injury and/or harm, including, but not  
4 limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic  
5 losses.  
6

7 170. Additionally, as a direct and proximate result of Defendant’s negligence, Plaintiff  
8 and the Class have suffered and will suffer the continued risks of exposure of their PII, which  
9 remain in Defendant’s possession and is subject to further unauthorized disclosures so long as  
10 Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued  
11 possession.  
12

13 171. Plaintiff and Class members are entitled to compensatory and consequential  
14 damages suffered as a result of the Data Breach.

15 172. Defendant’s negligent conduct is ongoing, in that it still holds the PII of Plaintiff  
16 and Class members in an unsafe and insecure manner.

17 173. Plaintiff and Class members are also entitled to injunctive relief requiring  
18 Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to  
19 future annual audits of those systems and monitoring procedures; and (iii) continue to provide  
20 adequate credit monitoring to all Class members.  
21

22 **COUNT II**  
23 **Breach Of Implied Contract**  
**(On Behalf of Plaintiff and the Class)**

24 174. Plaintiff restates and realleges paragraphs 1 through 137 above as if fully set forth  
25 herein.

26 175. Plaintiff and Class members were required to provide their PII to Defendant as a  
27 condition of receiving services and loyalty program membership from Defendant.  
28

3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102  
725-235-9750  
lasvegas@stranchlaw.com  
STRANCH, JENNINGS & GARVEY  
PLLC



1 176. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and  
2 the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard  
3 and protect such information, to keep such information secure and confidential, and to timely and  
4 accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.  
5

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

9 178. Implicit in the agreement between Plaintiff and Class members and the Defendant  
10 to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take  
11 reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide  
12 Plaintiff and Class members with prompt and sufficient notice of any and all unauthorized access  
13 and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class members  
14 from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such  
15 information secure and confidential.  
16

17 179. The mutual understanding and intent of Plaintiff and Class members on the one  
18 hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

19 180. Defendant solicited, offered, and invited Plaintiff and Class members to provide  
20 their PII as part of Defendant's regular business practices. Plaintiff and Class members accepted  
21 Defendant's offers and provided their PII to Defendant.  
22

23 181. In accepting the PII of Plaintiff and Class members, Defendant understood and  
24 agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

25 182. On information and belief, at all relevant times Defendant promulgated, adopted,  
26 and implemented written privacy policies whereby it expressly promised Plaintiff and Class  
27 members that it would only disclose PII under certain circumstances, none of which relate to the  
28



1 Data Breach.

2 183. On information and belief, Defendant further promised to comply with industry  
3 standards and to make sure that Plaintiff's and Class members' PII would remain protected.

4 184. Plaintiff and Class members paid money and provided their PII to Defendant with  
5 the reasonable belief and expectation that Defendant would use part of its earnings to obtain  
6 adequate data security. Defendant failed to do so.

7 185. Plaintiff and Class members would not have entrusted their PII to Defendant in the  
8 absence of the implied contract between them and Defendant to keep their information reasonably  
9 secure.

10 186. Plaintiff and Class members would not have entrusted their PII to Defendant in the  
11 absence of their implied promise to monitor their computer systems and networks to ensure that it  
12 adopted reasonable data security measures.

13 187. Plaintiff and Class members fully and adequately performed their obligations  
14 under the implied contracts with Defendant.

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

19 189. As a direct and proximate result of Defendant's breach of the implied contracts,  
20 Plaintiff and Class members sustained damages, as alleged herein, including the loss of the benefit  
21 of the bargain.

22 190. Plaintiff and Class members are entitled to compensatory, consequential, and  
23 nominal damages suffered as a result of the Data Breach.

24 191. Plaintiff and Class members are also entitled to injunctive relief requiring  
25  
26  
27  
28



1 Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit  
2 to future annual audits of those systems and monitoring procedures; and (iii) immediately provide  
3 adequate credit monitoring to all Class members.

4  
5 **COUNT III**  
6 **Unjust Enrichment**  
7 **(On Behalf of Plaintiff and the Class)**

8 192. Plaintiff restates and realleges paragraphs 1 through 137 above as if fully set forth  
9 herein.

10 193. This count is pleaded in the alternative to the Breach of Implied Contract claim  
11 above (Count II).

12 194. Plaintiff and Class members conferred a monetary benefit on Defendant.  
13 Specifically, they paid for services from and enrolled in loyalty program membership with  
14 Defendant and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class  
15 members should have received from Defendant the services that were the subject of the transaction  
16 and should have had their PII protected with adequate data security.

17 195. Defendant knew that Plaintiff and Class members conferred a benefit upon it and  
18 has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant  
19 profited from Plaintiff's retained data and used Plaintiff's and Class members' PII for business  
20 purposes.

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

23 197. Defendant acquired the PII through inequitable record retention as it failed to  
24 disclose the inadequate data security practices previously alleged.

25 198. If Plaintiff and Class members had known that Defendant would not use adequate  
26 data security practices, procedures, and protocols to adequately monitor, supervise, and secure their  
27  
28





1 PII, they would have entrusted their PII at Defendant or obtained loyalty program membership at  
2 Defendant.

3 199. Plaintiff and Class members have no adequate remedy at law.

4 200. Under the circumstances, it would be unjust for Defendant to be permitted to retain  
5 any of the benefits that Plaintiff and Class members conferred upon it.  
6

7 201. As a direct and proximate result of Defendant's conduct, Plaintiff and Class  
8 members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy;  
9 (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated  
10 with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the  
11 bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences  
12 of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a)  
13 remains unencrypted and available for unauthorized third parties to access and abuse; and (b)  
14 remains backed up in Defendant's possession and is subject to further unauthorized disclosures so  
15 long as Defendant fails to undertake appropriate and adequate measures to protect the PII.  
16

17 202. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages  
18 from Defendant and/or an order proportionally disgorging all profits, benefits, and other  
19 compensation obtained by Defendant from its wrongful conduct. This can be accomplished by  
20 establishing a constructive trust from which the Plaintiff and Class members may seek restitution  
21 or compensation.  
22

23 203. Plaintiff and Class members may not have an adequate remedy at law against  
24 Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the  
25 alternative to, other claims pleaded herein.  
26  
27  
28



**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and Class members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff’s and Class members’ PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:
  - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendant to protect, including through encryption, all data collected through the course of their 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 Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;

3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102  
725-235-9750  
lasvegas@stranchlaw.com  
STRANCH, JENNINGS & GARVEY  
PLLC

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class members;
- v. prohibiting Defendant from maintaining the PII of Plaintiff and Class members on a cloud-based database;
- vi. 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;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant’s network is compromised, hackers cannot gain access to other portions of Defendant’s systems;
- ix. requiring Defendant to conduct regular database scanning and securing checks;
- x. 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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

identifying information, as well as protecting the personal identifying information of Plaintiff and Class members;

- xi. 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;
- xii. 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;
- xiii. 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;
- xiv. 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;
- xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
- xvi. 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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

evaluate Defendant’s compliance with the terms of the Court’s final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court’s final judgment;

- D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;
- E. For an award of punitive damages, as allowable by law;
- F. For an award of attorneys’ fees and costs, and any other expenses, including expert witness fees;
- G. Pre- and post-judgment interest on any amounts awarded; and
- H. Such other and further relief as this court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury on all issues so triable.

Dated: September 21, 2023.

Respectfully submitted,

/s/ Nathan Ring

Nathan R. Ring  
**STRANCH, JENNINGS & GARVEY, PLLC**  
3100 W. Charleston Boulevard, Suite 208  
Las Vegas, NV 89102  
Telephone: (725) 235-9750  
nring@stranchlaw.com

Jeff Ostrow\*  
**KOPELOWITZ OSTROW**  
**FERGUSON WEISELBERG GILBERT**  
One West Las Olas Blvd., Suite 500  
Fort Lauderdale, Florida 33301  
Telephone: 954-525-4100  
ostrow@kolawyers.com

J. Gerard Stranch IV\*  
**STRANCH, JENNINGS & GARVEY, PLLC**  
The Freedom Center  
223 Rosa L. Parks Avenue, Suite 200

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Nashville, TN 37203  
Telephone: (615) 254-8801  
gstranch@stranchlaw.com

*Counsel for Plaintiff and the Proposed Class*

*\*Pro Hac Vice application forthcoming*

3100 W. Charleston Blvd., #208  
Las Vegas, NV 89102  
725-235-9750  
lasvegas@stranchlaw.com  
STRANCH, JENNINGS & GARVEY  
PLLC

