

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS**

MICHAEL GLEBIV, individually and on behalf of  
all others similarly situated,

Plaintiff,

v.

MIDWEST GAMING & ENTERTAINMENT,  
LLC d/b/a RIVERS CASINO,

Defendant.

Case No.: \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMAND**

Plaintiff Michael Glebiv (“Plaintiff”), individually and on behalf of all others similarly situated, brings this action against Defendant Midwest Gaming & Entertainment, LLC d/b/a Rivers Casino. (“Rivers Casino” or “Defendant”), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

**NATURE OF THE ACTION**

1. This is a data breach class action brought on behalf of consumers whose sensitive personal information was stolen by cybercriminals in a massive cyber-attack at Rivers Casino starting in August 2023 (the “Data Breach”).
2. Defendant is a casino, located in Des Plaines, Illinois, that offers gambling, dining, and other entertainment services to its customers.
3. Information stolen in the Data Breach included individuals’ sensitive information, including at least, full names, phone numbers, email addresses, dates of birth, driver’s licenses, government ID numbers, financial account numbers, tax identification numbers, passport numbers

and Social Security numbers (collectively, the “PII”).

4. Plaintiff and Class Members now face an ongoing and lifetime risk of identity theft, which is heightened by the exposure of their Social Security numbers to criminals.

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

6. Plaintiff’s and Class Members’ sensitive personal information—which was entrusted to Defendant, their officials and agents—was compromised, unlawfully accessed, and stolen due to the Data Breach.

7. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant’s inadequate safeguarding of Class Members’ PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

8. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant’s computer network in a condition vulnerable to cyberattacks of this type. On information and belief, the PII was kept unencrypted by Defendant as, had proper encryption been implemented, the criminals would have exfiltrated only unintelligible data.

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

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

11. Because of the Data Breach, Plaintiff and Class Members suffered injury and damages in the form of theft and misuse of their PII.

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

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

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

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

16. As a direct and proximate result of the Data Breach, Plaintiff and Class Members

have suffered and will continue to suffer damages and economic losses in the form of: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

17. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed and/or removed from the network during the Data Breach.

18. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief--including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring and identity restoration services funded by Defendant.

19. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct.

#### **PARTIES**

20. Plaintiff Michael Glebiv is a resident and citizen of Chicago, Illinois. Plaintiff Glebiv would not have entrusted his PII to Rivers Casino had he known that Rivers Casino would fail to maintain adequate data security. Plaintiff Glebiv's PII was compromised and disclosed as a result of the Data Breach.

21. Defendant Rivers Casino is a limited liability company organized under the laws of the state of Delaware with its principal place of business located at 900 North Michigan Avenue,

#1600, Chicago, Illinois 60611. Defendant is wholly owned by Midwest Gaming Borrower, LLC.

### **JURISDICTION AND VENUE**

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of \$5,000,000 exclusive of interest and costs, and members of the proposed Class are citizens of states different from Defendant.<sup>1</sup>

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

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District and a substantial part of the events and omissions giving rise to this action occurred in this District.

### **FACTUAL ALLEGATIONS**

#### ***Defendant's Business***

25. Defendant is a casino, located in Des Plaines, Illinois, that offers gambling, dining, and other entertainment services to its customers.

26. Plaintiff and Class Members are current and former customers and/or employees at Rivers Casino.

27. As a condition of obtaining entertainment products and/or services at Defendant,

---

<sup>1</sup> According to the breach report submitted to Commonwealth of Massachusetts, 1,821 Massachusetts residents were impacted in the Data Breach. See <https://www.mass.gov/doc/data-breach-report-2023/download>

Rivers Casino requires that its customers, including Plaintiff and some Class Members, entrust it with highly sensitive personal information. Similarly, as a condition of obtaining employment at Defendant, Rivers Casino requires that its employees, including some Class Members, entrust it with highly sensitive personal information.

28. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its services.

29. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

30. Upon information and belief, Defendant made promises and representations to its customers and employees, including Plaintiff and Class Members, that the PII collected from them as a condition of their employment at Defendant and/or as a condition of obtaining entertainment products and/or services at Defendant would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

31. Indeed, Defendant's Privacy Policy provides that: “[w]e use commercially reasonable measures to provide our Services.”<sup>2</sup>

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

33. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant

---

<sup>2</sup> <https://www.riverscasino.com/desplaines/privacy-policy>

to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

34. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

35. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

36. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

37. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

### ***The Data Breach***

38. On or about November 20, 2023, Defendant began sending Plaintiff and other Data Breach victims a Notice of Data Breach email (the "Notice Letter"), informing them that:

#### **WHAT HAPPENED?**

While our operations were not impacted, Rivers determined that this incident involved unauthorized access to our network. Specifically, on November 2, 2023, we determined that files containing certain personal information of Rivers Casino Des Plaines Team Members, customers, and online sportsbook customers may have been accessed or removed from our network as a result of this incident on or around August 12, 2023. We have not identified any indication that the networks of any other Rivers casinos were accessed during this incident. Further, no BetRivers online or mobile gaming platform, operations or systems were compromised or breached.



**WHAT INFORMATION WAS INVOLVED**

The affected information included name, contact information (such as phone number, email address, and postal address), date of birth, driver's license or government ID number. For a limited number of customers or Team Members, financial account number, tax identification number, Social Security number, and/or passport number was also affected.<sup>3</sup>

39. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

40. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

41. 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, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

42. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted PII of Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

43. Plaintiff further believes his PII and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

***Data Breaches Are Preventable***

---

<sup>3</sup> <https://www.riverscasino.com/desplaines/statements-and-releases-rivers-casino-des-plaines>



44. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

45. 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, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

46. The unencrypted PII of Class Members may end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

47. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”<sup>4</sup>

48. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

---

<sup>4</sup> How to Protect Your Networks from RANSOMWARE, at 3, *available at*: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.<sup>5</sup>

49. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

---

<sup>5</sup> *Id.* at 3-4.

**Thoroughly investigate and remediate alerts**

- Prioritize and treat commodity malware infections as potential full compromise;

**Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

**Build credential hygiene**

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

**Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

**Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].<sup>6</sup>

50. Given that Defendant was storing the PII of its current and former customers and current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

51. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach

---

<sup>6</sup> See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

and the exposure of the PII of, upon information and belief, tens of thousands of individuals, including that of Plaintiff and Class Members.

52. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

***Defendant Knew or Should Have Known of the Risk Because Casinos In Possession Of PII Are Particularly Susceptible To Cyber Attacks***

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

54. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

55. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.<sup>7</sup>

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

57. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so

---

<sup>7</sup> See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”<sup>8</sup>

58. Additionally, as companies became more dependent on computer systems to run their business,<sup>9</sup> *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.<sup>10</sup>

59. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

60. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

61. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including,

---

<sup>8</sup> [https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl\\_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=consumerprotection](https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection)

<sup>9</sup> <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

<sup>10</sup> <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

62. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to, upon information and belief, tens of thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

63. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

64. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

65. As a casino in possession of its current and former customers' and employees' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems, or those on which it transferred PII, were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

***Value of Personally Identifiable Information***

66. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”<sup>11</sup> The FTC describes “identifying information” as “any name or number that may be used, alone or

---

<sup>11</sup> 17 C.F.R. § 248.201 (2013).

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>12</sup>

67. 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>13</sup>

68. For example, PII can be sold at a price ranging from \$40 to \$200.<sup>14</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>15</sup>

69. Social Security numbers, which were compromised for some Class Members in the Data Breach, 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 some Class Members, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number

---

<sup>12</sup> *Id.*

<sup>13</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

<sup>14</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

<sup>15</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>



and assuming your identity can cause a lot of problems.<sup>16</sup>

70. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

71. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

72. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."<sup>17</sup>

73. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200."<sup>18</sup>

74. According to national credit bureau Experian:

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

---

<sup>16</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>

<sup>17</sup> *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, available at: <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658>

<sup>18</sup> <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658>

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

75. According to cybersecurity specialty publication CPO Magazine, “[t]o those unfamiliar with the world of fraud, driver’s license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation.”<sup>19</sup> However, this is not the case. As cybersecurity experts point out:

“It’s a gold mine for hackers. With a driver’s license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.”<sup>20</sup>

76. Victims of driver’s license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.<sup>21</sup>

77. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—names, dates of birth, and Social Security numbers.

78. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market.”<sup>22</sup>

---

<sup>19</sup> <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/>

<sup>20</sup> *Id.*

<sup>21</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>

<sup>22</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

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

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

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>23</sup>

***Defendant Fails to Comply with FTC Guidelines***

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

82. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

---

<sup>23</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>

is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

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

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

85. These enforcement actions include actions against entertainment companies, like Defendant.

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

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

***Defendant Failed to Comply with Industry Standards***

88. As noted above, experts studying cyber security routinely identify entertainment companies in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

89. Several best practices have been identified that a minimum should be implemented by entertainment companies in possession of PII, like Defendant, including but not limited to: educating all consumers; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which consumers can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

90. Other best cybersecurity practices that are standard in the entertainment industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

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

92. These foregoing frameworks are existing and applicable industry standards in the

entertainment industry. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

***Defendant's Breach***

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

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
  - b. Failing to adequately protect customers' and employees' PII;
  - c. Failing to properly monitor its own data security systems for existing intrusions, encryptions, brute-force attempts, and clearing of event logs;
  - d. Failing to apply all available security updates;
  - e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;
  - f. Failing to practice the principle of least-privilege and maintain credential hygiene;
  - g. Failing to avoid the use of domain-wide, admin-level service accounts;
  - h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;
  - i. Failing to properly train and supervise employees in the proper handling of inbound emails.
94. As the result of computer systems in dire need of security upgrading and inadequate

procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII.

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

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

***Common Injuries and Damages***

97. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

***The Data Breach Increases Victims' Risk Of Identity Theft***

98. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.



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

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

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

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

103. One such example of criminals piecing together bits and pieces of compromised PII

for profit is the development of “Fullz” packages.<sup>24</sup>

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

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

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

107. Thus, even if certain information (such as insurance information) was not stolen in

---

<sup>24</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a 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-/>(<https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/>

the data breach, criminals can still easily create a comprehensive “Fullz” package.

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

***Loss Of Time To Mitigate Risk Of Identity Theft And Fraud***

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

110. Thus, due to the actual and imminent risk of identity theft, Defendant’s Notice Letter instructs Plaintiff and Class Members to do the following: “this letter provides precautionary measures you can take to help protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant against incidents of identity theft and fraud and review your financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis.”<sup>25</sup>

111. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach as well as monitoring their financial accounts and credit reports for fraudulent activity, which may take years to detect.

---

<sup>25</sup> Notice Letter.

112. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>26</sup>

113. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>27</sup>

114. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>28</sup>

#### ***Diminution Value Of PII***

115. PII is a valuable property right.<sup>29</sup> Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison

---

<sup>26</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data 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>.

<sup>27</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

<sup>28</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

<sup>29</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, 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).

sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

116. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>30</sup>

117. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.<sup>31,32</sup>

118. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>33</sup>

119. Conversely sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.<sup>34</sup>

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

121. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

---

<sup>30</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

<sup>31</sup> <https://datacoup.com/>

<sup>32</sup> <https://digi.me/what-is-digime/>

<sup>33</sup> Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html>

<sup>34</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change, e.g., names, dates of birth, and Social Security numbers.

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

123. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

125. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s network, amounting to, upon information and belief, tens of thousands of individuals’ detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

126. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

***Future Cost of Credit & Identity Theft Monitoring is Reasonable and Necessary***

127. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong

probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims’ names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

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

129. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

130. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant’s Data Breach.

***Loss Of The Benefit Of The Bargain***

131. Furthermore, Defendant’s poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for entertainment products and/or services and/or accept an employment position at Defendant, Plaintiff and other reasonable consumers and employees understood and expected that they were, in part, paying for the entertainment products and/or services and/or being paid less for the necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received entertainment products and/or services and/or employment positions that were of a lesser value than what they reasonably expected to receive under the



bargains they struck with Defendant.

***Plaintiff Glebiv's Experience***

132. Plaintiff Michael Glebiv is a customer at Defendant who visited Rivers Casino in approximately 2021.

133. As a condition of obtaining entertainment products and/or services at Rivers Casino, Plaintiff was required to provide his PII to Defendant, including his name, date of birth, and Social Security number.

134. At the time of the Data Breach—on or around August 12, 2023—Defendant retained Plaintiff's PII in its system.

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

136. Plaintiff Michael Glebiv received the Notice Letter, by email, from Defendant, dated November 30, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his name and/or driver's license and/or government ID number.

137. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach as well as monitoring his financial accounts and credit reports for fraudulent activity, which may take years to detect. Plaintiff has spent significant time on activities in response to the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or

recreation. This time has been lost forever and cannot be recaptured.

138. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

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

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

142. Plaintiff Michael Glebiv has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

#### **CLASS ACTION ALLEGATIONS**

143. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully

set forth herein.

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

145. Plaintiff proposes the following Class definition, subject to amendment as appropriate

**Nationwide Class**

All persons in the United States whose PII was maintained on Defendant's computer systems that were compromised in the Data Breach including those who were sent Notice of Data Breach Incident emails from Defendant (the "Class").

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

147. Plaintiff reserves the right to amend the definitions of the Class and/or add a Class if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

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

149. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. Although the precise number is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, tens of thousands of individuals' PII was compromised in the Data Breach.

150. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common

questions of law and fact include, without limitation:

- a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;
- b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the cyber-attack;
- c) Whether Defendant's data security systems prior to and during the cyber-attack complied with applicable data security laws and regulations;
- d) Whether Defendant's data security systems prior to and during the cyber-attack were consistent with industry standards;
- e) Whether Defendant owed a duty to Class Members to safeguard their PII;
- f) Whether Defendant breached its duty to Class Members to safeguard their PII;
- g) Whether computer hackers obtained Class Members' PII in the cyber-attack;
- h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j) Whether Defendant owed a duty to provide Plaintiff and Class Members notice of this data breach, and whether Defendant breached that duty;
- k) Whether Defendant's conduct was negligent;
- l) Whether Defendant's acts, inactions, and practices complained of herein

amount to an invasion of privacy;

- m) Whether Defendant's actions violated federal law; and
- n) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

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

152. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

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

154. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendant.

In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

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

**COUNT I**  
**Negligence**  
**(On Behalf of Plaintiff and All Class Members)**

156. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

157. Plaintiff and the Class entrusted Defendant with their PII on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

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

159. By collecting and storing this data on Defendant's computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

160. Defendant owed a duty of care to Plaintiff and Class Members to provide data

security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

161. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and the individuals who entrusted them with PII, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

162. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure. In addition,

163. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

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

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

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;



- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to have in place mitigation policies and procedures;
- d. Allowing unauthorized access to Class Members' PII;
- e. Failing to detect in a timely manner that Class Members' PII had been compromised; and,
- f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

166. Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

167. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

168. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and Class Members' injuries-in-fact.

169. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols.

170. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures

to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

171. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act WAS intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statute intended to guard against.

172. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

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

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

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

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

177. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing

adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

178. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

179. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

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

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

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

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

184. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated

with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

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

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

187. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

188. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

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

adequate credit monitoring to all Class Members.

**COUNT II**  
**Negligence *Per Se***  
**(On Behalf of Plaintiff and All Class Members)**

190. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

191. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

192. Defendant's failure to comply with the FTC Act and similar state statutes and regulations constitutes negligence *per se*.

193. Plaintiff and Class Members are within the class of persons that the Federal Trade Commission Act intended to protect, and the type of harm that resulted from the Data Breach was the type of harm that the Federal Trade Commission Act intended to guard against.

194. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

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

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

**COUNT III**  
**Breach Of Implied Contract**

**(On Behalf of Plaintiff and All Class Members)**

197. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

198. When Plaintiff and Class Members provided their PII to Defendant as a condition of their employment at Defendant and/or to obtain entertainment products and/or services at Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to destroy any PII that it was no longer required to maintain.

199. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

200. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

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

202. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including the FTC Act, and were consistent with industry standards.

203. Plaintiff and Class Members paid money and/or provided their labor as well as provided their PII to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

204. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably

secure.

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

206. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

207. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII or to destroy it once it was no longer necessary to retain the PII.

208. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

209. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

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

**COUNT IV**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff and All Class Members)**

211. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

212. This Count is pleaded in the alternative to the breach of contract count above.

213. Upon information and belief, Defendant funds its data security measures entirely



from their general revenue, including payments made by Plaintiff and the Class Members.

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

215. Plaintiff and Class Members conferred a monetary benefit upon Defendant. Specifically, they provided their labor to Defendant and/or purchased entertainment products and/or services from Defendant and/or their agents and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the employment position and/or entertainment products and/or services that were the subject of the transaction and have their PII protected with adequate data security.

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

217. Defendant was enriched by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid the data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

219. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

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

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

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

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

**COUNT V**  
**Violation Of The Illinois Consumer Fraud Act**  
**815 Ill. Comp. Stat. §§ 505/1, et seq.**  
**(On Behalf of Plaintiff and All Class Members)**

225. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

226. Plaintiff and the Class are “consumers” as that term is defined in 815 ILL. COMP. STAT. § 505/1(e).

227. Plaintiff, the Class, and Defendant are “persons” as that term is defined in 815 ILL. COMP. STAT. § 505/1(c).

228. Defendant is engaged in “trade” or “commerce,” including the provision of services, as those terms are defined under 815 ILL. COMP. STAT. § 505/1(f).

229. Defendant engages in the “sale” of “merchandise” (including services) as defined by 815 ILL. COMP. STAT. § 505/1(b) and (d).

230. Defendant’s acts, practices, and omissions were done in the course of Defendant’s business of marketing, offering for sale, and selling entertainment products and/or services in the State of Illinois.

231. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of “merchandise” (as defined in the Illinois CFA) in violation of the Illinois CFA, including, but not limited to, the following:

- a. failure to maintain adequate computer systems and data security practices to safeguard current and former customers' and employees' PII;
- b. failure to disclose the material fact that its computer systems and data security practices were inadequate to safeguard the personal information it was collecting and maintaining from theft;
- c. failure to disclose in a timely and accurate manner to Plaintiff and the Class

Members the material fact of Defendant's data breach;

- d. misrepresenting material facts to Plaintiff and the Class, in connection with the sale of goods and services, by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class members' PII from unauthorized disclosure, release, data breaches, and theft;
- e. misrepresenting material facts to the class, in connection with the sale of goods and services, by representing that Defendant did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class members' PII, and
- f. failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Class members' PII from further unauthorized disclosure, release, data breaches, and theft.

232. In addition, Defendant's failure to disclose that its computer systems were not well protected and that Plaintiff's and Class members' sensitive information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Defendant knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and the Class; and (b) defeat Plaintiff's and Class members' ordinary, foreseeable and reasonable expectations concerning the security of their PII on Defendant's servers.

233. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with Defendant's offering of goods and services and storing Plaintiff's and Class members' PII on its servers, in violation of the Illinois CFA.

234. Defendant also engaged in unfair acts and practices by failing to maintain the

privacy and security of Class Members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach.

235. These unfair acts and practices violated duties imposed by laws including Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

236. Defendant's wrongful practices occurred in the course of trade or commerce.

237. Defendant's wrongful practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendant that applied to all Class Members and were repeated continuously before and after Defendant obtained PII from Plaintiff and Class members.

238. All Class members have been adversely affected by Defendant conduct and the public was and is at risk as a result thereof.

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

240. Pursuant to 815 ILL. COMP. STAT. § 505/10a(a), Plaintiff seeks actual, compensatory, and punitive damages (pursuant to 815 ILL. COMP. STAT. § 505/10a(c)),

injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the Illinois CFA.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grants the following:

- A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of 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 its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
  - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of 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;
  - iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

- v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;
- xi. requiring Defendant to conduct regular database scanning and securing checks;
- xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a



- breach;
- xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
  - xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
  - xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
  - xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
  - xviii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;
  - E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
  - F. For prejudgment interest on all amounts awarded; and
  - G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands that this matter be tried before a jury.

Date: November 27, 2023

Respectfully Submitted,

/s/Gary M. Klinger

Gary M. Klinger

**MILBERG COLEMAN BRYSON**

**PHILLIPS GROSSMAN, LLC**

227 W. Monroe Street, Suite 2100

Chicago, IL 60606

Tel.: (866) 252-0878

Email: [gklinger@milberg.com](mailto:gklinger@milberg.com)

*Attorney for Plaintiff and the Putative Class*

