John J. Nelson (SBN: 317598)
**MILBERG, PLLC**
280 S. Beverly Drive-Penthouse
Beverly Hills, CA 90212
Tel: (858) 209-6941
jnelson@milberg.com

*Counsel for Plaintiff and the Putative Class*

**UNITED STATES DISTRICT COURT**
**CENTRAL DISTRICT OF CALIFORNIA**

| | |
|---|---|
| ISIAH RAMOS, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>LIVE NATION ENTERTAINMENT, INC.,<br><br>Defendant. | Case No.<br><br>**CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

Plaintiff Isiah Ramos ("Plaintiff"), by and through undersigned counsel, on behalf of himself and all others similarly situated ("Class Members"), alleges the following Class Action Complaint (the "Action") against Defendant Live Nation Entertainment, Inc. ("Defendant") upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

## I. SUMMARY

1. Plaintiff brings this Action on behalf of himself and all other similarly situated victims as a result of a recent cyberattack and data breach involving personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") suffered by Defendant, which Defendant reported to the Office of the Vermont Attorney general on October 1, 2026[1] (the "Data Breach").

2. Defendant is the world's leading entertainment company and operates as a global live entertainment promoter and venue management firm, selling live event tickets and hosting concerts and live performances across the world.[2]

3. Plaintiff and Class Members impacted by the Data Breach provided their Private Information to Defendant in connection with the services Defendant provides.

4. At least the following types of Private Information were compromised as a result of the Data Breach: Social Security numbers, Government ID numbers, and health records.[3]

5. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect individuals' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

[1] https://ago.vermont.gov/categories/security-breach-notices (last visited, Oct. 6, 2026).
[2] https://www.livenationentertainment.com/ (last visited Oct. 6, 2026).
[3] https://ago.vermont.gov/categories/security-breach-notices (last visited, Oct. 6, 2026).

6. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class Members' Private Information was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all persons whose Private Information was exposed as a result of the Data Breach.

7. Upon information and belief, Plaintiff's Private Information is available on the dark web as a result of the Data Breach.

8. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

9. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members notice of the Data Breach.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (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) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, 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 Private Information.

11. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself, and all similarly situated individuals whose Private Information was accessed during the Data Breach.

12. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence/negligence *per se*, (ii) breach of implied contract, and (iii) unjust enrichment.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

## II. JURISDICTION AND VENUE

14. This Court has jurisdiction over the subject matter of this Action pursuant to 28 U.S.C. § 1332(d), as provided by the Class Action Fairness Act,

because: this is a civil action filed under Rule 23 of the Federal Rules of Civil Procedure; the amount in controversy exceeds $5,000,000, exclusive of interest and costs; the proposed Class consists of more than 100 members; and at least one member of the Class is a citizen of a different state than Defendant, namely Plaintiff, a citizen of Illinois.

15. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business within this District, because Defendant resides in and regularly transacts business in the State of California, and because a substantial part of the events, omissions, and acts giving rise to this Action occurred in the State of California.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant resides in this District, and pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

## III. PARTIES

***Plaintiff***

17. Plaintiff is an individual citizen and resident of Champaign, Illinois.

***Defendant***

18. Defendant is a corporation organized under the laws of the State of Delaware, maintaining its principal place of business at 9348 Civic Center Drive, Beverly Hills, CA 90210.

## IV. FACTUAL ALLEGATIONS

***Defendant's Business***

19. Defendant is the world's leading entertainment company and operates as a global live entertainment promoter and venue management firm, selling live event tickets and hosting concerts and live performances across the world.[4]

20. Defendant collects personally identifiable information in the course of doing business. This personally identifiable information includes the Private Information of Plaintiff and Class Members which was compromised in the Data Breach alleged herein. But for Defendant's collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to provide its services.

21. Upon information and belief, Defendant promises to maintain the confidentiality of Plaintiff's and Class Members' Private Information to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiff's and Class Members' Private Information for non-essential purposes.

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

23. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members would not have entrusted Defendant with their Private Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

24. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

[4] https://www.livenationentertainment.com/ (last visited Oct. 6, 2026).

***The Attack and Data Breach***

25. On or around October 1, 2026, Defendant reported the Data Breach to the Office of the Vermont Attorney General.[5]

26. Plaintiff and Class Members impacted by the Data Breach provided their Private Information to Defendant in connection with the services Defendant provides.

27. At least the following types of Private Information were compromised as a result of the Data Breach: Social Security numbers, Government ID numbers, and health records.[6]

28. Due to Defendant's inadequate security measures, Plaintiff and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

29. Upon information and belief, the Private Information was not encrypted prior to the Data Breach.

30. Upon information and belief, the cyberattack was targeted at Defendant as a company that collects and maintains valuable personal data from a significant number of individuals in connection with providing its services, including Plaintiff and Class Members.

31. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the Private Information of Plaintiff and Class Members.

32. Defendant had obligations to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

---

[5] https://ago.vermont.gov/categories/security-breach-notices (last visited, Oct. 6, 2026).
[6] *Id.*

33. Plaintiff and Class Members provided their Private Information 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.

34. Upon information and belief, and through its privacy policy ("Privacy Policy"),[7] Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

***The Data Breach Was Foreseeable and Defendant Was Aware of the Risk***

35. It is well known that Private Information, including Social Security numbers and PHI in particular, is an invaluable commodity and a frequent target of hackers.

36. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

37. In 2023, a record 3,205 data breaches occurred in the United States, resulting in about 349,221,481 sensitive records being exposed, a greater than 100%

[7] **https://privacy.livenation.com/privacy-policy?_gl=1*69deq7*_ga*MTczMzkyNjQ4Ny4xNzkxMzE4ODc1** ("Any information collected by us or our third-party partners in compliance with applicable health and safety requirements, will only be used to contact attendees or shared with relevant local, government officials. This information is regularly deleted… We have security measures in place to protect your information… We only keep your information for as long as required to provide you with the services you request, for the purposes outlined in this policy and for any legal purposes for which we are obliged to keep the information… We will securely delete your information when it is no longer required for these purposes, in line with our company policies… When transferring information, there are strict rules in place to ensure your information is still protected to the highest standard. Where we do this, we will ensure that appropriate safeguards are put in place.") (last visited Oct. 6, 2026).

increase from 2019.[8] These statistics have held steady for 2024 – when 3,158 data compromises occurred.[9]

38. Individuals place a high value not only on their Private Information, but also on the privacy of that data. For the individual, identity theft causes significant negative financial impact on victims as well as severe distress and other strong emotions and physical reactions.

39. In light of recent high profile data breaches at other industry leading companies, including, T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), LoanDepot (16.9 million affected, January 2024), Evolve Bank & Trust (7.6 million affected, May 2024), Financial Business and Consumer Solutions (4.2 million affected, February 2024), and Prudential Financial (2.5 million affected, February 2024), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

40. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

41. Additionally, as companies became more dependent on computer systems to run their business, *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is

[8] ITRC (Identity Theft Resource Center), *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/ (last visited Oct. 6, 2026).

[9] ITRC (Identity Theft Resource Center), *2024 Data Breach Report* (January 2025), *available at* https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited Oct. 6, 2026).

magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.

42. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information 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.

43. 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, thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

44. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duties to keep the Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and the proposed Class from being compromised.

***Defendant Could Have Prevented the Data Breach***

45. Data breaches are preventable.[10] "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[11] "Organizations that collect,

[10] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.

[11] *Id.* at 17.

use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[12]

46. Most reported data breaches "are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[13]

47. Here, many failures laid the groundwork for the Data Breach.

48. The Federal Trade Commission ("FTC") has published guidelines that establish reasonable data security practices for businesses.[14]

49. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[15]

50. The FTC guidelines establish that businesses should protect the confidential 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 for installing vendor-approved patches to correct security problems.[16]

51. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic

---

[12] *Id.* at 28.
[13] *Id.*
[14] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf.
[15] *Id.*
[16] *Id.*

for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[17]

52. According to information and belief, Defendant failed to follow reasonable and necessary industry standards to prevent a data breach, including the FTC's guidelines.

53. Defendant was at all times fully aware of its obligation to protect the Private Information of consumers under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

54. Based on allowing its security certificates to lapse and upon information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

55. 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."[18]

---

[17] *Id.*

[18] *See 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.

56. To prevent and detect the attack here, Defendant could and should have taken, as recommended by the Federal Bureau of Investigation, the following measures:

- Implemented 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.
- Enabled 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.
- Scanned all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configured firewalls to block access to known malicious IP addresses.
- Patched 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.
- Managed 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.
- Configured 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.

- Disabled 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.
- Implemented 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.
- Considered disabling Remote Desktop protocol (RDP) if it is not being used.
- Used application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Executed operating system environments or specific programs in a virtualized environment.
- Categorized data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[19]

57. According to information and belief, Defendant failed to do any of the above.

58. To prevent and detect cyberattacks, Defendant could and should have required individuals, as recommended by the United States Cybersecurity & Infrastructure Security Agency, to take the following measures:

[19] *Id.* at 3–4.

- **Updated and patched your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Used caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).
- **Opened email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Kept your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it.
- **Verified email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group

website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Used and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[20]

59. In addition, to prevent and detect the Data Breach Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Harden internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audits
- **Thoroughly investigate and remediate alerts.**
  - Prioritize and treat commodity malware infections as potential full compromise of the system
- **Include IT professionals in security discussions.**
  - Ensure collaboration among security operations, security administrators, and information technology administrators to configure servers and other endpoints securely
- **Build and maintain credential hygiene**

[20] *See Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (revised Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (internal citations omitted).

- Use multifactor authentication or network level authentication and enforce strong, randomized, just-in-time local administrator 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**
  - Utilize 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[21]

60. Specifically, among other failures, Defendant had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[22]

61. Moreover, it is well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed.[23]

---

[21] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT THREAT INTELLIGENCE (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[22] *See* Adnan Raja, *How to Safeguard Your Business Data With Encryption*, DATAINSIDER (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

[23] *See Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

62. The FTC has repeatedly emphasized the importance of disposing of unnecessary Private Information: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[24] Rather than following this basic standard of care, Defendant kept thousands of individuals' unencrypted Private Information on its inadequately secured systems indefinitely.

63. In sum, the Data Breach could have been easily prevented through standard practices like the use of industry standard network segmentation, redaction, and encryption of all Private Information—which Defendant negligently failed to do.

64. Further, the scope of the Data Breach could have been dramatically reduced had Defendant utilized proper record retention and destruction practices—but Defendant negligently did no such thing.

***Defendant Had a Duty to Plaintiff and Class Members to Secure Private Information***

65. At all relevant times, Defendant had a duty to Plaintiff and Class Members to properly secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when Defendant became aware that their Private Information may have been compromised.

66. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and

[24] *Id.* at 6.

Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class relied on Defendant to secure their Private Information when they entrusted Defendant with the information required in connection with the services Defendant provides.

67. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

68. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for Private Information;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

69. The ramifications of Defendant's failure to keep Private Information secure are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims is likely to continue for years.

***The Value of Personally Identifiable Information***

70. The Private Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, [25] and bank details can have a price range of $30 to over $4,000.[26]

71. As a growing number of federal courts have begun to recognize the loss of value of Private Information as a viable damages theory, the sale of Private Information from data breaches, as in the Data Breach alleged herein, is particularly harmful to data breach victims – especially when it takes place on the dark web.

72. The dark net is an unindexed layer of the internet that requires special software or authentication to access.[27] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[28] This prevents dark web marketplaces from being easily identifiable to authorities or those not in the know.

---

[25] *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/ (last visited Oct. 6, 2026).

[26] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 6, 2026).

[27] *What Is the Dark Web?,* Experian, *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited Oct. 6, 2026).

[28] *Id.*

73. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, sensitive personal information like the Private Information at issue here.[29] The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth and other personal information.[30] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others." [31]

74. Plaintiff's and Class Members' Private Information is a valuable commodity, a market exists for Plaintiff's and Class Members' Private Information (which is why the Data Breach was perpetrated in the first place), and Plaintiff's and Class Members' Private Information is likely being sold by hackers on the dark web (as that is the *modus operandi* of data thieves) – as a result, Plaintiff and Class Members have lost the value of their Private Information, which is sufficient to plausibly allege injury arising from a data breach.

75. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[32] In fact,

---

[29] *What is the Dark Web?* – Microsoft 365, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited Oct. 6, 2026).
[30] *Id.*; *What Is the Dark Web?,* Experian, *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited Oct. 6, 2026).
[31] *What is the Dark Web?* – Microsoft 365, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited Oct. 6, 2026).
[32] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Oct. 6, 2026).

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.[33] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60.00 a year.[34]

76. The Private Information stolen in this specific Data Breach was particularly harmful.

77. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular personal privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including: 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts," and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity Theft, which involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft; and 5) Utility Fraud.

78. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud. Social Security numbers, which were compromised in the Data Breach, are among the worst kinds of private information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

[33] https://datacoup.com/ (last visited Oct. 6, 2026).
[34] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Oct. 6, 2026).

79. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [35] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[36]

80. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and 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, when 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 and assuming your identity can cause a lot of problems.[37]

81. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[38] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for

---

[35] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases. (last visited Oct. 6, 2026)

[36] *Id.*

[37] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 6, 2026)

[38] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited Oct. 6, 2026)

jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[39]

82. 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.

83. 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."[40]

84. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff's Social Security

[39] *See* https://www.investopedia.com/terms/s/ssn.asp (last visited Oct. 6, 2026)

[40] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Oct. 6, 2026).

numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target him in fraudulent schemes and identity theft attacks.")

85. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[41]

86. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web.

87. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[42]

88. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive

---

[41] *Medical I.D. Theft*, EFraudPrevention https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected. (last visited Oct. 6, 2026).

[42] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed Oct. 6, 2021)

director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[43]

89. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[44] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[45]

90. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[46]

91. Given the nature of Defendant's Data Breach, as well as Defendant's failure to notify Plaintiff and Class Members, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and

---

[43] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed Oct. 6, 2026).
[44] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Oct. 6, 2026).
[45] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/ (last accessed Oct. 6, 2026).
[46] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

Class Members' Private Information can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

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

***The Harm Caused by the Data Breach Now and Going Forward***

93. Victims of data breaches are susceptible to becoming victims of identity theft for years to come. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9).

94. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft and Plaintiff and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

95. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web, where malicious actors buy and sell that information for profit.[47]

96. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity.[48] Marketplaces similar to the

[47] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Oct. 6, 2026).

[48] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018) https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited Oct. 6, 2026).

now-defunct AlphaBay continue to be "awash with [Private Information] belonging to victims from countries all over the world."[49]

97. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information 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.

98. 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.

99. 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.

100. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[50]

---

[49] *Id.*

[50] "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 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

101. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information 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.

102. The development of "Fullz" packages means here that the stolen Private Information 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 Private Information 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.

***Loss of Time to Mitigate the Risk of Identity Theft and Fraud***

103. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[51] Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen.

---

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-firm/.(last visited Oct. 6, 2026).

[51] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited Oct. 6, 2026).

Defendant did not notify impacted people for over four months after learning of the Data Breach.

104. 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 Private Information 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.

105. 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 contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

106. These efforts are consistent with the U.S. Government Accountability Office, which 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."[52]

107. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert

[52] *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. (last visited Oct. 6, 2026).

(and considering 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.[53]

***Diminution of Value of Private Information***

108. Private Information is a valuable property right.[54] The value is axiomatic, considering the value of Big Data in corporate America, and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that Private Information has considerable market value.

109. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, 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 Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

110. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's

---

[53] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps. (last visited Oct. 6, 2026).

[54] *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). (last visited Oct. 6, 2026).

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.

111. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

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

112. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

113. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information 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 Private Information for identity theft crimes.

114. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

115. As a result, Plaintiff and Class Members also request relief in the form of the future cost of credit and identity theft monitoring, which is reasonable and necessary. 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 and protect Class Members from the risk of identity theft that arose from the Data Breach.

***Loss of the Benefit of the Bargain***

116. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide their Private Information to Defendant, Plaintiff and other reasonable consumers understood and expected that in exchange, Defendant would implement necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

***Plaintiff's Experience***

117. Plaintiff provided his Private Information to Defendant in connection with obtaining services from Defendant.

118. Plaintiff learned of the Data Breach after reading an article online.

119. Upon information and belief, Plaintiff's Private Information was on Defendant's system before, after, and during the Data Breach. As a result, Plaintiff is a victim of the Data Breach.

120. To date, Defendant has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach particularly given the fact that Plaintiff's Private Information has already been impacted in the Data Breach and likely been made available on the dark web to anyone wishing to purchase it.

121. Nor has Defendant compensated Plaintiff and Class Members for the time they will spend monitoring their accounts, placing credit freezes and fraud alerts, changing online passwords and other actions.

122. Plaintiff and Class Members have been further damaged by the compromise of their Private Information in the Data Breach which was impacted and is in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the Private Information.

123. Plaintiff typically takes measures to protect his Private Information and is very careful about sharing his Private Information. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

124. Plaintiff stores any documents containing his Private Information in a safe and secure location, and he diligently chooses unique usernames and passwords

for his online accounts.

125. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In response to the Data Breach, Plaintiff has spent time monitoring his accounts and credit score, verifying the legitimacy of the Data Breach, and on other necessary mitigation efforts. This is time that was lost and unproductive and took away from other activities and duties.

126. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his Private Information — a form of intangible property that he entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

127. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

128. Plaintiff suffered emotional distress and increased stress and anxiety as a result of the Data Breach because of the actions he has been forced to undertake, the loss of control over his most intimate information, and the fact that he must remain vigilant for the remainder of his life.

129. Plaintiff has suffered imminent and impending injury arising from the increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

130. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Defendant acquired Plaintiff's Private Information. Plaintiff, however, would not have entrusted his Private

Information to Defendant had he known that it would fail to maintain adequate data security. Plaintiff's Private Information was compromised and disclosed as a result of the Data Breach.

131. 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. 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.

## V. CLASS ACTION ALLEGATIONS

132. Plaintiff brings this class action, individually and on behalf of the following classes under Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3):

> Nationwide Class
> All persons residing in the United States whose Private Information was compromised as a result of the Data Breach, including all persons who received Defendant's Notice (the "Class").

133. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

134. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

135. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

136. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates that the Class is comprised of at least thousands of members. The Class is sufficiently numerous to warrant certification.

137. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class Members, had his Private Information compromised because of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the members of the Class. The harms suffered by Plaintiff are similar to those suffered by all other Class Members, which were caused by the same misconduct by Defendant.

138. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, or in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

139. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing

as asserted herein.

140. Commonality and Predominance: Defendant engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' Private Information was stored on the same network and unlawfully accessed in the same way. There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b) Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c) Whether Defendant's storage of Plaintiff's and Class Members' Private Information was done in a negligent manner;

d) Whether Defendant had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;

e) Whether Defendant's conduct was negligent;

f) Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;

g) Whether Defendant took sufficient steps to secure individuals' Private Information; and

h) The nature of relief, including damages, to which Plaintiff and Class Members are entitled.

141. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage

since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

142. Manageability: The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

143. Ascertainability: Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

144. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief and corresponding declaratory relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

145. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses.

## VI. CAUSES OF ACTION

### COUNT I
### NEGLIGENCE/NEGLIGENCE *PER SE*
### (On Behalf of Plaintiff and the Class)

146. Plaintiff hereby repeats and realleges paragraphs 1 through 145 of this Complaint and incorporates them by reference herein.

147. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information for pecuniary gain, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

148. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

149. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed. The harm that Plaintiff and Class Members experienced was within the zone of foreseeable harm known to Defendant.

150. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a mandatory step in obtaining services from Defendant. While this special relationship exists independent from any contract, it is recognized by Defendant's privacy practices, as well as applicable laws and regulations. Specifically, Defendant actively solicited and gathered Private

Information as part of its business and was solely responsible for and in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a resulting data breach.

151. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

152. 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 and the frequency of data breaches in general.

153. Defendant also had a common law duty to prevent foreseeable harm to others. Plaintiff and the Class were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of adequately safeguarding that Private Information, and the necessity of encrypting Private Information stored on Defendant's systems. It was foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

154. Defendant's conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry

standards for the safekeeping of Plaintiff's and the Class's Private Information, including basic encryption techniques available to Defendant.

155. Plaintiff and the Class had and have no ability to protect their Private Information that was in, and remains in, Defendant's possession.

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

157. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

158. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

159. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

160. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information

within Defendant's possession might have been compromised and precisely the type of information compromised.

161. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

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

163. The FTCA is intended, in part, to protect individuals whose Private Information is maintained by another and who are unable to safeguard their information as they cannot exercise control or direction over the data security practices.

164. Plaintiff and the members of the Class are within the class of persons that the FTCA was intended to protect as their Private Information was collected and maintained by Defendant and they were unable to exercise control over Defendant's data security practices.

165. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against.

166. 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 members of the Class.

167. Defendant breached its duties to Plaintiff and the members of the Class under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

168. Had Plaintiff and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiff and the members of the Class would not have entrusted Defendant with their Private Information.

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

170. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the members of the Class, they would not have been injured.

171. The injury and harm suffered by Plaintiff and the members of the Class 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 the members of the Class to experience the foreseeable harms associated with the exposure of their Private Information.

172. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiff's and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains 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 Private Information in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of Private Information as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

173. As a direct and proximate result of Defendant's negligence and negligence *per se*, 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.

174. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains 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 Private Information in its continued possession.

175. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are now at an increased risk of identity theft or fraud.

176. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is entitled to and demands actual, consequential, and nominal damages and injunctive relief to be determined at trial.

## COUNT II
## BREACH OF IMPLIED CONTRACT
## (On Behalf of Plaintiff and the Class)

177. Plaintiff hereby repeats and realleges paragraphs 1 through 145 of this Complaint and incorporates them by reference herein.

178. Plaintiff and the Class entrusted their Private Information to Defendant in connection with the services Defendant provides. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

179. At the time Defendant acquired the Private Information of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the Private Information and not take unjustified risks when storing the Private Information.

180. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide Private Information was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

181. Plaintiff and the Class would not have entrusted their Private Information to Defendant had they known that Defendant would make the Private Information internet-accessible, not encrypt sensitive data elements, and not delete

the Private Information when Defendant no longer had a reasonable need to maintain it.

182. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

183. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

184. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

185. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

## COUNT III
## UNJUST ENRICHMENT
## (On Behalf of Plaintiff and the Class)

186. Plaintiff hereby repeats and realleges paragraphs 1 through 145 of this Complaint and incorporates them by reference herein.

187. This Count is brought in the alternative to Count II, Breach of Implied Contract.

188. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant with their valuable Private Information. In so conferring this benefit, Plaintiff and Class Members understood that part of the benefit Defendant derived from the Private Information would be applied to data security efforts to safeguard the Private Information.

189. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

190. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its 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.

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

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

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

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

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

196. 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.

197. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

## VII. PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff, individually and on behalf of the Class defined herein, prays for judgment as against Defendant as follows:

a.) For an Order certifying this action as a Class action 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 Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c.) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d.) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e.) Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

f.) For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined, as allowable by law;

g.) For an award of punitive damages, as allowable by law;

h.) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i.) Pre- and post-judgment interest on any amounts awarded and,

j.) All such other and further relief as this court may deem just and proper.

**JURY TRIAL DEMAND**

Plaintiff hereby demands a trial by jury.

DATED: October 7, 2026

Respectfully submitted,

*/s/ John J. Nelson*

John J. Nelson (SBN: 317598)
**MILBERG, PLLC**
280 S. Beverly Drive-Penthouse
Beverly Hills, CA 90212
Tel: (858) 209-6941
jnelson@milberg.com

*Attorney for Plaintiff and the Class*