UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO

JACK KRABBE, individually and on behalf of all others similarly situated, Plaintiff, v. OAK VIEW GROUP, LLC, Defendant.	**Case No.:** **CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Jack Krabbe, individually and on behalf of all others similarly situated, brings this class action against Oak View Group, LLC ("OVG" or "Defendant") and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the personally identifiable information ("PII" or "Private Information") of Plaintiff and other similarly situated employees of Defendant ("Class Members").

2. Defendant is Delaware Corporation headquartered in Denver, Colorado and is a hospitality and entertainment management company that employs thousands of individuals in multiples states.[1]

[1] *Who We Are*, OAK VIEW GRP., https://www.oakviewgroup.com/who-we-are/ (last visited June 22, 2026).

3. On or around June 2026, OVG filed official notice of a hacking incident with the Office of the Texas Attorney General.[2]

4. Upon information and belief, Defendant experienced a data breach between December 16, 2025, and January 16, 2026, when an unauthorized third party gained access to OVG's computer systems and exfiltrated certain files that contained Plaintiff's and Class Members' highly sensitive and confidential PII (the "Data Breach").[3]

5. The PII impacted by the Data Breach includes, but is not limited to, names, addresses, social security numbers, and tax identification numbers.[4]

6. The PII compromised in the Data Breach is precisely the type of data that is highly coveted by cybercriminals and identity thieves. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain financial services, 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.

7. The fact that an unauthorized actor removed the PII, as Defendant itself has acknowledged, means that the data was not merely accessed or viewed but was affirmatively exfiltrated from Defendant's systems. This exfiltration dramatically increases the risk that the data

---

[2] *Data Breach Security Reports*, TEX. ATT'Y GEN., https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited June 22, 2026); *see also 2026-975- Oak View Group, LLC*, MASS ATT'Y GEN. (June 15, 2026) https://www.mass.gov/doc/2026-975-oak-view-group-llc.

[3] *2026-975- Oak View Group, LLC*, MASS ATT'Y GEN. (June 15, 2026) https://www.mass.gov/doc/2026-975-oak-view-group-llc.

[4] *See supra* note 2.

has been, or will be, sold, published, or used for identity theft, fraud, phishing, social engineering, and other malicious purposes. Once removed by an unauthorized actor, there is no mechanism to retrieve, recall, or "un-steal" the data.

8. Defendant further compounded Plaintiff's and Class Members' injuries by delaying notification of the Data Breach for over five months after detection, depriving affected individuals of the opportunity to take prompt protective action during the critical period immediately following the breach.

9. Moreover, there has been no assurance offered by Defendant that any personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. As a direct and proximate result of Defendant's failures, Plaintiff and Class Members have suffered and will continue to suffer injuries, including but not limited to: (a) the unauthorized exfiltration and exposure of their PII; (b) loss of the benefit of the bargain and employment that did not include adequate data protection; (c) loss of the value of their privacy and confidentiality in their PII; (d) the present and continuing heightened risk of identity theft, medical identity fraud, insurance fraud, and other crimes, including increased spam emails; (e) time and money expended and to be expended mitigating the consequences of the Data Breach; (f) anxiety, emotional distress, and loss of privacy; and (g) diminution of the value of their PII.

11. Plaintiff brings this action to hold Defendant accountable and to obtain damages, restitution, and injunctive and declaratory relief requiring Defendant to implement and maintain reasonable data security practices, including encryption, multi-factor authentication, regular penetration testing, and appropriate access controls, and to provide adequate credit monitoring and identity theft protection services to Plaintiff and Class Members, among other relief.

PARTIES

12. Plaintiff Jack Krabbe is a resident and citizen of Baltimore Maryland.

13. Defendant Oak View Group, LLC, is a hospitality and entertainment company organized in Delaware with its headquarters located at 5050 S. Syracuse Street, Suite 800, Denver, Colorado 80237. Defendant's registered agent, National Registered Agents, Inc., can be found at 7700 E Arapahoe Rd Ste 220, Centennial, Colorado 80112

JURISDICTION AND VENUE

14. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from OVG.[5] Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

15. This Court has jurisdiction over OVG because OVG is headquartered and conducts business in this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because OVG resides in this District and is being served in this District.

[5] Indeed, Plaintiff is a citizen of Maryland. *See also supra* note 2.

COMMON FACTUAL ALLEGATIONS

A. Defendant's Collection and Storage of PII

17. Defendant is Delaware Corporation headquartered in Denver, Colorado and operates its a hospitality and entertainment management company that employs thousands of individuals around the world.[6]

18. As a condition of employment with OVG, Defendant requires that its employees entrust it with highly sensitive personal information. In the ordinary course of employment with OVG, Plaintiff and Class Members were required to provide their PII to Defendant, including their full names, dates of birth, addresses, phone numbers, email addresses, and Social Security numbers.

19. Upon information and belief, 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, who are past and current employees of Defendant.

20. Defendant made promises and representations to Plaintiff and Class Members that their PII would be kept safe and confidential, and that the privacy of that information would be maintained.

21. Plaintiff and Class Members provided their PII to Defendant with the reasonable understanding and expectation that Defendant would comply with applicable laws, regulations, and industry standards to keep such information confidential and protected from unauthorized access. Defendant received significant economic value from the receipt and use of Plaintiff's and Class Members' PII.

---

[6] *Who We Are*, OAK VIEW GRP., https://www.oakviewgroup.com/who-we-are/ (last visited June 22, 2026).

22. As a result of collecting and storing the PII of Plaintiff and Class Members for their own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures and adequate security to protect Plaintiff's and the Class Members' PII from unauthorized disclosure to third parties.

23. On information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect Plaintiff's and Class Members' PII or supervised its providers and employees to prevent, detect, and stop breaches of their network or systems. As a result, Defendant leaves significant vulnerabilities in their systems for cybercriminals to exploit and gain access to Plaintiff's and Class Members' PII.

B. The Data Breach

24. Defendant experienced a data breach between December 16, 2025, and January 16, 2026, when an unauthorized third party gained access to OVG's computer systems and exfiltrated certain files that contained Plaintiff's and Class Members' highly sensitive and confidential PII.[7]

25. Despite the Data Breach occurring at least as early as December 16, 2025, OVG did not discover the Data Breach until January 19, 2026.[8]

26. Following discovery of the breach, Defendant launched an investigation that determined "an unauthorized third party gained access to a subset of OVG's legacy systems . . . and leveraged that access to remove certain files from OVG's network."[9]

27. On or around June 12, 2026, Defendant began notifying the impacted individuals and Attorneys General around the Country about the data breach (the "Notice").[10]

---

[7] *2026-975- Oak View Group, LLC*, MASS ATT'Y GEN. (June 15, 2026) https://www.mass.gov/doc/2026-975-oak-view-group-llc.
[8] *Id.*
[9] *Id.*
[10] *See supra* note 2.

28. The PII impacted by the Data Breach includes, but is not limited to, names, addresses, social security numbers, and tax identification numbers.[11]

29. Omitted from the Notice was the identity of the cybercriminals who perpetrated this Data Breach, 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.

30. 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.

31. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice, including (a) that this Data Breach was the work of cybercriminals; (b) that the cybercriminals first infiltrated Defendant's legacy systems and downloaded data (a.k.a. exfiltrated data, or in layperson's terms, "stole" data); and (c) that once inside Defendant's systems, the cybercriminals targeted information including Plaintiff's and Class Members' PII.

32. Moreover, despite learning of the Data Breach on or around January 19, 2025, Defendant waited until on or about June 12, 2026, before notifying victims of the Data Breach.

33. This timeline betrays a shockingly ill-prepared cybersecurity posture, particularly because Colo. Rev. Stat. § 6-1-716 mandates that following discovery or notification of a breach, disclosure of the data breach shall be made within 30 calendar days of discovery or notification of the data breach.

34. Defendant's prolonged investigation and response time, in addition to the *modus*

[11] *Id.*

operandi to use a double-extortion model,[12] strongly suggests either (i) Defendant only discovered the Data Breach upon delivery of a ransom note after the cybercriminals completed most of its attack, or (ii) Defendant discovered the attack prior to the ransom note but could not prevent cybercriminals from accessing and exfiltrating PII.

35. Given that the hackers were able to infiltrate Defendant's legacy systems for an extended period of time and perform malicious activity—including reconnaissance and data exfiltration functions that should have had alarm bells ringing—it is likely that Defendant failed to implement reasonable industry standard cybersecurity safeguards sufficient to detect malicious activity in a timely manner, including monitoring, logging, and alerting systems such as EDR, XDR, data loss prevention tools, and centralized alerting and logging.

36. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to Plaintiff's and Class Members' PII.

37. Given Defendant's failure in even the most basic requirements of cybersecurity, it is likely that Defendant's cybersecurity program as a whole is severely inadequate in comparison to the measures it is legally obligated to provide to individuals for whom it collects PII, thus leaving them exposed to the Data Breach that indeed came into fruition.

C. Defendant's Data Breach Was Imminently Foreseeable

38. Defendant was on notice that companies in the its industry are susceptible targets for data breaches.

39. It is well known that PII is an invaluable commodity and a frequent target of

[12] *#Stop Ransomware Guide*, CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last visited June 22, 2026).

hackers.

40. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years. In light of past high profile data breaches at industry-leading companies, including, for example, 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, if acting as a reasonable business, should have known that the PII it collected and maintained would be vulnerable to and targeted by cybercriminals.

41. In 2024, 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[13]

42. 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. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[14]

43. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the industry, including Defendant.

44. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its

---

[13] *2024 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter. org/publication/2024-data-breach-report/ (last visited June 22, 2026).

[14] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 22, 2026).

own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

45. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included extortion and threatening to release stolen data.

46. In light of the information readily available and accessible before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Data breaches are so prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

D. Value of Personally Identifiable Information

47. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

48. The PII of individuals remains of high value to criminals, as evidenced by the prices

[15] 17 C.F.R. § 248.201 (2013).
[16] *Id.*

they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[17]

49. The information compromised in the Data Breach is even more significant because it includes Social Security numbers, which are extraordinarily sensitive and private and is commonly used to perpetrate fraud.

50. 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."[18]

51. 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.[19]

E. Defendant Failed to Comply with FTC Guidelines

52. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need

---

[17] Anita George, *Your Personal Data Is for Sale on The Dark Web. Here's How Much It Costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.

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

[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

53. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information 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 is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

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

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by 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 the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. Such FTC enforcement actions include those against businesses that fail to adequately protect employee data, like Defendant here. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

57. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

58. Defendant was at all times fully aware of its obligation to protect the PII of consumers under the FTC Act 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 PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

F. Defendant Failed to Comply with Industry Standards.

59. Experts studying cybersecurity routinely identify institutions that store PII like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

60. To prevent and detect unauthorized cyber-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.

- 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 at least privilege in mind. If a user only needs to read specific files, the user should not have written 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.[20]

61. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch 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 . . . .

- **Use 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) . . . .

- **Open 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.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it . . . .

- **Verify 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.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network

[20] HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE 3–4, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (U.S. Government Interagency technical guidance document)(last visited June 22, 2026).

traffic . . . .[21]

62. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, 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;

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

63. Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[22]

---

[21] *Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (April 11, 2019), https://www.cisa.gov/news-events/news/protecting-against-ransomware (revised Sept. 2, 2021).

[22] *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.

64. Some industry best practices that should be implemented by institutions dealing with sensitive PII, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its timeline, Defendant failed to follow some or all of these industry best practices.

65. Other best cybersecurity practices that are standard at large institutions that store PII include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

66. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

67. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

68. Common Injuries & Damages

69. Because 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: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); and (d) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

i. The Data Breach Increases Victims' Risk of Identity Theft and Fraud

70. Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because Defendant's failures resulted in Plaintiff's and Class Members' PII falling into the hands of identity thieves.

71. The unencrypted PII of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the PII for the express purpose of conducting financial fraud and identity theft operations.

72. Further, the standard operating procedure for cybercriminals is to use some data, like the PII here, to access "Fullz packages" of that person to gain access to the full suite of additional PII that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types

of attacks.[23]

73. 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 to assemble complete dossiers on individuals.

74. 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.

75. Individuals, like Plaintiff and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hackers' purposes.

76. According to the Social Security Administration, each time an individual's Social

[23] "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 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://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

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."[24] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[25]

> 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 and assuming your identity can cause a lot of problems.[26]

77. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[27] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[28]

78. Identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

---

[24] *See Avoid Identity Theft*, SOC. SEC. ADMIN., https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases

[25] *Id.*

[26] *Identity Theft and Your Social Security Number*, SOC. SEC. ADMIN. (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[27] *See How to Protect Yourself from Social Security Number Identity Theft*, EQUIFAX, https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited June 22, 2026).

[28] *See* Julia Kagan, *What is an SSN? What to Know About Social Security Numbers*, INVESTOPEDIA (Sept. 2, 2024) https://www.investopedia.com/terms/s/ssn.asp.

79. Such fraud may go undetected until debt collection calls commence months, or even years later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

80. Data Breach victims suffer long-term consequences when their social security numbers are taken and used by hackers. Even if they know their social security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

81. 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.

82. 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."[29]

83. Similarly, the Social Security Administration has warned that "a new number

[29] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other PII, such as your name and address, remains the same."[30]

84. Further, the California state government states that "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[31]

85. The FTC recommends that identity theft victims take several costly steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.[32]

86. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein.

87. Defendant knew or should have known of these harms which would be caused by

---

[30] *Identity Theft and Your Social Security Number*, Pub. No. 05-10064, SOCIAL SEC. ADMIN. (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[31] *See Your Social Security Number: Controlling the Key to Identity Theft*, CAL. DEPT. JUST. https://oag.ca.gov/idtheft/facts/your-ssn
[32] *What To Do Right Away*, FTC (2024), https://www.identitytheft.gov/Steps.

the Data Breach they permitted to occur and strengthened its data systems accordingly.

ii. Loss of Time to Mitigate Risk of Identity Theft and Fraud

88. Because 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 of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendant arguing that the individual failed to mitigate damages.

89. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff's and Class Members' PII is affected because such information is commonly used to commit medical and insurance fraud.

90. By spending this time, data breach Plaintiff is not manufacturing his own harm but is taking necessary steps at Defendant's direction and because the Data Breach included his PII.

91. 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 because 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 account statements for any indication of fraudulent activity, which may take years to detect.

92. 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."[33]

93. 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 (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.[34]

iii. The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

94. Based on the value of the information stolen, the data either has or will be sold to cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

95. 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.

96. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per 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. This is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

---

[33] *See* U.S. Gov't 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.

[34] *See* Fed. Trade Comm'n, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.

iv. Diminution in Value of PII

97. PII are valuable property rights.[35] Their value is axiomatic, considering the value of Big Data in corporate America and that cyber theft convictions include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

98. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[36]

99. 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.[37]

100. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[38]

101. Conversely, sensitive PII can sell from any as little as $1 to more than $4,000 on the dark web according to Experian.[39]

102. 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

---

[35] *See, e.g.*, Randall T. Soma *et al*., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("Private Information, 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).

[36] David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, L.A. TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[37] *See e.g.*, https://datacoup.com/ (last visited June 22, 2026).

[38] *Frequently Asked Questions*, NIELSON COMPUT. & MOBIL PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited June 22, 2026).

[39] *See* Ben Luthi, *Here's What Your Data Sells for on the Dark Web*, EXPERIAN (June 30. 2025), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

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, PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

103. Additionally, Plaintiff and Class Members further seek to recover the value of the unauthorized access to their PII caused by Defendant's wrongful conduct. This measure of damages is analogous to remedies for the unauthorized use of intellectual property. Like technology protected by a trade secret, a person's PII is non-rivalrous — the unauthorized use by a third party does not diminish the owner's own ability to use such information, yet the owner may recover the reasonable value of its use, i.e., a "reasonable royalty," from the unauthorized user. A similar royalty or license measure of damages is appropriate here because: (a) Plaintiff and Class Members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, including evidence regarding the price at which similar data is transacted on both legitimate and illegitimate markets.

v. *Lost Benefit of the Bargain*

104. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide Defendant with their PII under certain terms, Plaintiff and Class Members understood and expected that Defendant would properly safeguard and protect their PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received employment of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Experience

105. Plaintiff is a former employee of Defendant and provided his Private Information to Defendant as a condition of receiving employment from Defendant.

106. At the time of the Data Breach, Defendant retained Plaintiff's PII in its system.

107. Upon information and belief, Plaintiff's PII was compromised in the Data Breach and stolen by cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting Private Information.

108. Plaintiff is very careful about sharing his sensitive PII/PHI. 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.

109. In order to obtain employment from Defendant, Plaintiff was required to provide his Private Information to Defendant, including among other things, his name, contact information, date of birth, Social Security number, Driver's license, Passport, emergency contact information, and financial account information.

110. As a result of the Data Breach, Plaintiff made and will continue to make reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. As such, Plaintiff has spent significant time dealing with 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.

111. Plaintiff suffered actual injury from having his PII compromised as a result of the

Data Breach including, but not limited to: (i) misuse of Private Information; (ii) spam calls and communications; (iii) invasion of privacy; (iv) theft of his PII; (v) lost or diminished value of PII; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; (viii) statutory damages; (ix) nominal damages; and (x) 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.

112. Plaintiff suffered actual injury from the dramatic increase in spam, suggesting that his PII has been stolen and is now in the hands of cybercriminals.

113. 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 his of key details about the Data Breach's occurrence.

114. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

115. 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.

116. Plaintiff 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.

117. Plaintiff greatly values his privacy, and would not have provided his Private Information, undertaken the employment that he did if he had known that his Private Information would be maintained using inadequate data security systems

CLASS ALLEGATIONS

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

119. Specifically, Plaintiff propose the following Class (referred to herein as the "Class"), subject to amendment as appropriate:

> All individuals residing in the United States whose PII was compromised in the Data Breach, including all who were sent a notice of the Data Breach (the "Class").

120. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

121. Plaintiff reserves the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

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

123. 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:

- Whether Defendant engaged in the conduct alleged herein;
- Whether Defendant's conduct violated the FTC Act;

- When Defendant learned of the Data Breach;
- Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;
- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;
- Whether Defendant owed duties to Class Members to safeguard their PII;
- Whether Defendant breached its duties to Class Members to safeguard their PII;
- Whether hackers obtained Class Members' PII via the Data Breach;
- Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;
- Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;
- What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;
- Whether Defendant's conduct was negligent;
- Whether Defendant breached contracts it had with its employees, which were made expressly for the benefit of Plaintiff and Class Members;
- Whether Plaintiff and Class Members are entitled to damages;
- Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and among other things,
- Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

124. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

125. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

126. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated 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.

127. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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 claims 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, conducting 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.

128. Class certification is also appropriate. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

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

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE AND NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

130. Plaintiff incorporates the above allegations as if fully set forth herein.

131. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, 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.

132. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training employees and others who accessed PII within computer systems on how to adequately protect PII.

133. Defendant has a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

134. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

135. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' PII within their possession was compromised and precisely the types of information that were compromised.

136. Defendant owes a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected individuals' PII.

137. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. Defendant is in a position to ensure that its systems are sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

138. 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 is bound by industry standards to protect confidential PII.

139. Defendant has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendant is obligated to act with reasonable care to protect against these foreseeable threats.

140. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII.

141. 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 Plaintiff's and Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems and to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee information; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

d. Failing to detect the breach at the time it began or within a reasonable time thereafter; and

e. Failing to follow their own privacy policies and practices published to their employees and residents.

142. Further, Defendant's violation of federal statutes and other applicable laws also constitutes negligence *per se*. Specifically, as described herein, Defendant violated the FTC Act.

143. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff's and Class Members' PII. Various FTC publications and orders also form the basis of Defendant's standard of care.

144. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and by failing to comply with industry standards.

145. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

146. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty 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 suffered by Plaintiff and

Class Members.

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

148. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent the dissemination of Plaintiff's and Class Members' PII.

149. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

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

151. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in injuries to Plaintiff and Class Members.

152. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

153. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

154. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their PII had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

155. As a result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the emp[loyment bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff's and Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' PII.

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

156. Plaintiff incorporates the above allegations as if fully set forth herein.

157. Plaintiff and the Class were required to deliver their PII to Defendant as part of the process of obtaining employment provided by Defendant.

158. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their PII in exchange for employment. Plaintiff and Class Members accepted Defendant's offer and provided their PII to Defendant.

159. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately

notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

160. In providing their PII, Plaintiff and Class Members entered into an implied contract with Defendant. Pursuant to these implied contracts, Plaintiff and the Class understood that Defendant, in receiving such data, (1) provide employment to Plaintiff and Class Members, (2) take reasonable measures to safeguard Plaintiff's and the other Class Members' PII, (3) provide prompt and adequate notice of all unauthorized access and/or theft of their PII, and (4) protect Plaintiff's and Class Members' PII in compliance with federal and state laws and regulations and industry standards.

161. In delivering their PII to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

162. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

163. Defendant accepted possession of Plaintiff's and Class Members' PII.

164. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure employee PII, Plaintiff and members of the Class would not have provided their PII to Defendant.

165. Defendant recognized that Plaintiff's and Class Members' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

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

167. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard its data.

168. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their PII.

169. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the employment bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff's and Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' PII.

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

170. Plaintiff incorporates the above allegations as if fully set forth herein.

171. This claim is pleaded in the alternative to the breach of implied contractual duty

claim.

172. Upon information and belief, Defendant funds their data security measures entirely from its general revenues, including from general revenues generated by Plaintiff and Class Members on Defendant's behalf.

173. As such, Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant with their valuable PII as a portion of value and monies derived from Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each made that is allocated to data security is known to Defendant.

174. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

175. 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.

176. 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.

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

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

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

180. 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 PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which 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 PII 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 PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Member

181. 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.

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

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

183. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

184. Plaintiff and Class Members successfully took reasonable and appropriate steps to

keep their PII confidential from the public.

185. Defendant owed a duty to Plaintiff and the Class to keep their PII confidential.

186. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

187. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant in order to receive employment, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

188. Defendant's conduct also represents a public disclosure of private facts in that the disclosure was made to cybercriminals—individuals in a special relationship with Plaintiff and the proposed Class in that they are the exact group from whom the expected cybersecurity measures are intended to protect Plaintiff and the proposed Class.

189. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

190. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

191. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

192. By intentionally failing to keep Plaintiff's and Class Members' PII safe, and by

intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

193. As the Restatement explains, as used throughout the Restatement of Torts, intent "has reference to the consequences of an act rather than the act itself." Restatement (Second) of Torts § 8A, cmt. A (1964). "Intent is not, however, limited to consequences which are desired. If the actor knows that the consequences are certain, or substantially certain, to result from her act, and still goes ahead, she is treated by the law as if she had in fact desired to produce the result." *Id.* cmt. B.

194. Indeed, given the foreseeability of the harms inherent in data breaches and the ubiquitous nature of data breaches, Defendant was substantially certain that its failure to implement reasonable cybersecurity standards would lead to an invasion of Plaintiff's privacy.

195. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

196. As a proximate result of Defendant's acts and omissions, the PII of Plaintiff and the Class was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

197. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class because their PII is still maintained by Defendant with its inadequate cybersecurity system and

policies.

198. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

199. In addition to injunctive relief, Plaintiff, on behalf of himself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

PRAYER FOR RELIEF

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

A. For an Order certifying this action as a class action and appointing Plaintiff and 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' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

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

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

ii. requiring Defendant to protect, including through encryption, all data collected through the course of 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 implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

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

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

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

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

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

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

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

xiv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xv. for a period of 7 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 actual damages, compensatory damages, and nominal damages, in an amount to be determined, and for punitive damages, as allowable by law;

E. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

F. Pre- and post-judgment interest on any amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

Dated: June 22, 2026

Respectfully submitted,

/s/ Grayson Wells

J. Gerard Stranch, IV
Grayson Wells
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel.: (615) 254-8801
gwells@stranchlaw.com
gstranch@stranchlaw.com

Counsel for Plaintiff and the Proposed Class