IN THE STATE COURT OF FULTON COUNTY
STATE OF GEORGIA

HARLEY BLANDFORD and **JULIE HARDIN**, individually and on behalf of all others similarly situated, Plaintiffs, v. **NTH DEGREE, INC.**, Defendant.	Case No.: **DEMAND FOR A JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiffs Harley Blandford and Julie Hardin ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant Nth Degree, Inc. ("Nth Degree" or "Defendant") individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Plaintiffs' and Class Members' sensitive information, including their first and last name, address, date of birth, social security number, state identification number/ driver's license number, bank account information, and health information (the "Private Information").

2. Nth Degree, based in Duluth, Georgia, is a company that specializes in global marketing, trade shows, and event marketing and management serving thousands of individuals

3. Plaintiffs and Class Members (defined below), including Defendant's current and former customers, contractors, and employees, entrusted their Private Information to Defendant on the mutual understanding that Defendant would protect it against disclosure.

4. However, between December 12, 2024, and December 20, 2024, Defendant allowed an unauthorized party to access and retrieve Defendant's files containing Plaintiffs' and Class Members' Private Information (the "Data Breach").

5. As a result of the Data Breach, Plaintiffs and Class Members were, and continue to be, at significant and imminent risk of identity theft and various other forms of personal, social, and financial harm now and for the remainder of their respective lifetimes.

6. The Private Information compromised in the Data was a gold mine of highly sensitive and valuable information that is now in the hands of cyber-criminals who target, steal, and sale Private Information to identity thieves.

7. Armed with the Private Information accessed in the Data Breach, data thieves can and likely will 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 medical 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.

8. There has been no assurance offered by Nth Degree that all 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.

9. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable, concrete losses including, but not limited to: (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: remains unencrypted and available for unauthorized third parties to access and abuse and also 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.

10. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect consumers' Private Information from a foreseeable and preventable cyber-attack.

11. Moreover, upon information and belief, Defendant was targeted for a cyber-attack due to its status as a global leader in experiential marketing that collects and maintains highly valuable Private Information on its systems.

12. Defendant maintained, used, and shared the Private Information in a reckless manner. In particular, the Private Information was used and transmitted by Defendant in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take

steps necessary to secure the Private Information from those risks left the Private Information in a dangerous condition.

13. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

14. Upon information and belief, Nth Degree and its employees failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had Nth Degree properly monitored its networks; it would have discovered the Breach sooner.

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

16. Plaintiffs and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft and fraud.

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

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

19. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and, therefore, they are entitled to injunctive and other equitable relief.

20. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and declaratory judgment.

THE PARTIES

21. Plaintiff Harley Blandford is a resident and citizen of California.

22. Plaintiff Julie Hardin is a resident and citizen of Louisiana.

23. Defendant Nth Degree is incorporated in Delaware with its principal place of business in Duluth, Georgia.

JURISDICTION AND VENUE

24. This Court has personal jurisdiction over Defendant, as Defendant has sufficient minimum contacts with the State of Georgia. Through its business operations in the State of Georgia and in Fulton County, Defendant intentionally avails itself of the markets within this County to render the exercise of jurisdiction by this Court just and proper. Defendant does business in the State of Georgia and the business being done in Georgia directly relates to the subject of this lawsuit, thus rendering the exercise of personal jurisdiction by this Court proper and necessary.

25. Venue is proper because a substantial part of the business, events, and omissions giving rise to these claims occurred in Fulton County.

FACTUAL ALLEGATIONS

Defendant's Business and Collection of Private Information

26. Plaintiffs and Class Members are current or former clients, customers, contractors, and employees of Nth Degree.

27. Nth Degree is a global event marketing and management company specializing in trade shows, retail, and corporate events.[1] Founded in 1979, Nth Degree has 20 locations serving more than 450 cities in the United States and internationally.[2] Nth Degree employs more than 600 people and generates approximately $145 million in annual revenue.[3]

28. As a condition of receiving marketing and management services, Nth Degree requires that its clients, including Plaintiffs and Class Members, entrust it with highly sensitive personal information, including Social Security numbers, state identification and driver's license numbers, bank account information, and health information.

29. In the ordinary course of receiving services from Nth Degree, Plaintiffs and Class Members were required to provide their Private Information to Defendant, and they did so with the understanding that Nth Degree would protect their Private Information from unauthorized disclosure and use.

30. In its privacy policy, Nth Degree informs its clients that it "respect[s] and value[s] your privacy." Nth Degree states that "[w]e take what we believe to be reasonable steps to protect the Personal Information collected by us from loss, misuse, unauthorized use, access, inadvertent disclosure, alteration, and destruction."

[1] *See* https://www.nthdegree.com/services/ (last visited Dec. 11, 2025).
[2] *Id.*
[3] See https://growjo.com/company/Nth_Degree (last visited Dec. 11, 2025).

31. Because of the highly sensitive and personal nature of the information Nth Degree acquires and stores with respect to its clients, Nth Degree, upon information and belief, promises to, among other things: keep clients' Private Information private; comply with industry standards related to data security and the maintenance of its clients' Private Information; inform its clients of its legal duties relating to data security and comply with all federal and state laws protecting clients' Private Information; only use and release clients' Private Information for reasons that relate to the services it provides; and provide adequate notice to clients if their Private Information is disclosed without authorization.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Nth Degree 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 and exfiltration.

The Data Breach

33. On or about April 14, 2025, Defendant began sending Plaintiffs and other Data Breach victims an untitled letter (the "Notice Letter"), informing them that:

> *What Happened?*
>
> We recently discovered that an unauthorized party gained access to our network environment.
>
> *What Are We Doing?*
>
> Upon learning of this issue, we immediately worked to contain the threat and secure our network environment. We commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal or sensitive data had been accessed or acquired as a result of this incident. After an extensive forensic investigation and manual document review, we discovered on March 24, 2025 that your personal information may have been

> accessed or acquired by an unauthorized party between on or around December 12, 2024, to on or around December 20, 2024.[4]
>
> *What Information Was Involved?*
>
> The information potentially involved included your first and last name, address, date of birth, social security number, state identification number/driver's license number, bank account information, and health information.

34. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

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

36. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiffs' and Class Members' Social Security numbers for download and theft.

[4] The "Notice Letter". A redacted sample copy is available at chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mass.gov/doc/2025-681-nth-degree-investment-group/download

37. Companies only send notice letters because data breach notification laws require them to do so. And such letters are only sent to persons when Defendant has a reasonable belief that those persons' confidential information was accessed or acquired by an unauthorized individual or entity. Defendant cannot hide behind legalese – by sending a notice of data breach letter to Plaintiffs and Class Members, it admits that Defendant itself has a reasonable belief that Plaintiffs' and Class Members' names, Social Security numbers, and other sensitive information was accessed or acquired by an unauthorized actor – aka cybercriminals.

38. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

39. Defendant had obligations created by the FTC Act, HIPAA, contract, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

40. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

41. An unauthorized person accessed and acquired files containing the unencrypted Private Information of Plaintiffs and Class Members in the Data Breach.

42. Plaintiffs further believe that their Private Information and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

43. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

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

45. 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."[5]

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

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

[5] 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

- 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 files, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[6]

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

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management

[6] *Id.* at 3-4.

- 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
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[7]

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

49. The occurrence of the Data Breach shows that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in data thieves

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

acquiring the Private Information of, upon information and belief, tens of thousands of individuals, including that of Plaintiffs and Class Members.

Defendant Knew, Or Should Have Known, of the Risk Because Global Marketing Companies in Possession of Private Information Are Particularly Susceptible To Cyber Attacks

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

51. Data breaches, including those perpetrated against Global Marketing companies that store Private Information in their systems, have become widespread.

52. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims. The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78-percentage point increase over the previous year and a 72-percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

53. In light of recent high profile data breaches at other industry leading companies, including National Public Data (2.9 billion records, August 2024), Ticketmaster Entertainment, LLC (560 million records, May 2024), Change Healthcare Inc. (145 million records, February 2024), Dell Technologies, Inc. (49 million records, May 2024), and AT&T Inc. (73 million records, April 2024), Defendant knew or should have known that the Private Information it they collected and maintained would be targeted by cybercriminals.

54. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a

warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

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

56. Defendant knew and understood unprotected or exposed Private Information in the custody of companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

57. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs 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 Plaintiffs and Class Members as a result of a breach.

58. Plaintiffs and Class Members now face years of doing constant surveillance of their financial and personal records to avoid additional harm from the Data Breach. The Class is

[8]https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection

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

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

incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

59. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

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

61. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as victims of data breaches commonly face multiple *years* of ongoing identity theft and financial fraud, and credit monitoring entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information and the inevitable injuries they now face.

62. Defendant's offer of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive Private Information was in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

63. As a Global Marketing company possessing its customers' and employees' Private Information, Defendant knew, or should have known, of the importance of safeguarding Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Private Information

64. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] 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."[12]

65. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[13]

66. For example, Personal Information can be sold at a price ranging from $40 to $200.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

67. 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 person 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

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id.*
[13] *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/
[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

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.

68. 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 are among the worst kind 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.

69. 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." [16] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[17]

70. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

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

[16] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.
[17] *Id.*

> illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

71. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[19] "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."[20]

72. What's more, it is not an 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.

73. 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."[21]

74. 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-

[18] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf
[19] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/
[20] *See* https://www.investopedia.com/terms/s/ssn.asp
[21] 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-millionsworrying-about-identity-theft

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 Plaintiffs' Social Security 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 their in fraudulent schemes and identity theft attacks.")

75. Similarly, the California state government warns consumers 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."[22]

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

77. 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,

[22] *See* https://oag.ca.gov/idtheft/facts/your-ssn

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[23]

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

79. 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 Private Information 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.[24]

80. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendant Fails to Comply with FTC Guidelines

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

---

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

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

82. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[25]

83. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[26]

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

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

---

[25] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[26] *Id.*

86. These FTC enforcement actions include actions against Global Marketing companies, like Defendant.

87. 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 businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

88. Defendant failed to properly implement basic data security practices.

89. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information of its customers or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

90. Upon information and belief, Defendant was at all times fully aware of their obligation to protect the Private Information of its customers, Defendant was also aware of the significant repercussions that would result from their 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 Plaintiffs and the Class.

Defendant Fails to Comply with HIPAA Regulations.

91. Defendant is a covered businesses under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"),

and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

92. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

93. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

94. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

95. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information ["PHI"]." 45 C.F.R. § 164.302.

96. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

97. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity or business associate creates, receives, maintains, or transmits.

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

98. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

99. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

100. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

101. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. See 45 C.F.R. § 164.530(f).

102. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services (HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. See 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed

guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.

Defendant Fails to Comply with Industry Standards

103. As noted above, experts studying cyber security routinely identify Global Marketing companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

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

105. Other best cybersecurity practices that are standard for Global Marketing companies include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security

systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

106. 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.

107. These foregoing frameworks are existing and applicable industry standards for Global Marketing companies, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries & Damages

108. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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.

Data Breaches Increase Victims' Risk of Identity Theft

109. 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.

110. The unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers, if it has not been listed on the dark web already.

111. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply put, from now on, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

112. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

113. In fact, state legislatures have passed laws in recognition of these risks: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be

used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[27]

114. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[28]

115. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity after the initial account setup[.]"[29] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"[30]

116. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[31]

---

[27] *See* N.C. Gen. Stat. § 132-1.10(1).

[28] *See* https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers

[29] *See* https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/

[30] *See* https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/

[31] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground*

117. 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.

118. 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 Plaintiffs' 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.

119. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiffs and the other Class Members.

120. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

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

Loss Of Time to Mitigate Risk of Identity Theft & Fraud

122. As a result of the recognized risk of identity theft, when a Data Breach occurs, an individual is notified by a company that their Private Information was compromised, as in this

---

Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

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 – yet the resource and asset of time has been lost.

123. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiffs and Class Members to take the following measures to protect themselves: "…placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, we recommend that you always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."[32]

124. In addition, Defendant's Notice letter includes multiple pages that recommend Plaintiffs and Class Members to participate in activities such monitoring their accounts, placing security freezes and fraud alerts on their accounts, and contacting consumer reporting bureaus.[33]

125. Defendant's extensive suggestion of steps that Plaintiffs and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant time that Plaintiffs and Class Members must undertake in response to the Data Breach. Plaintiffs' and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiffs and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendant's Notice Letter.

---

[32] *See* Sample Redacted Notice Letter chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mass.gov/doc/2025-681-nth-degree-investment-group/download.; *See also* Exhibit A.

[33] *Id.*

126. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach. Accordingly, the Data Breach has caused Plaintiffs and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

127. Plaintiffs' mitigation 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."[34]

128. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

129. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

[34] *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.
[35] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

Diminution of Value of Private Information

130. Private Information is a valuable property right.[36] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

131. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[37]

132. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[38]

133. 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.[39,40, 41]

134. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[42]

135. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and

---

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

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

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

[39] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[40] https://datacoup.com/

[41] https://digi.me/

[42] https://www.thepennyhoarder.com/make-money/nielsen-panel/

diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs 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.

136. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs 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 Plaintiffs and Class Members as a result of a breach.

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

138. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

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

140. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

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

141. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, 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 –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

142. Such fraud may go undetected until debt collection calls commence months, or even years later. An individual may not know that his or their Private Information 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.

143. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

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

Lost Benefit of The Bargain

145. Furthermore, Defendant's poor data security practices deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for Global Marketing services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for all attendant services, including necessary data security to protect their Private Information that they were required to provide.

146. Yet, Defendant did not provide the expected data security.

147. Accordingly, Plaintiffs 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.

Plaintiffs' Experiences

Plaintiff Harley Blandford

148. Plaintiff Harley Blandford is a former customer of Nth Degree who was required to provide his Private Information to Nth Degree to obtain services.

149. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Blandford's Private Information in its system.

150. Plaintiff Blandford is very careful about sharing his sensitive Private Information. Plaintiff Blandford stores any documents containing his Private Information in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

151. Plaintiff Blandford learned of the data breach after reviewing the Notice. According to the Notice, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties. The Private Information comprised some combination of his name, address, date of birth, social security number, state identification number/driver's license number, bank account information and health information.

152. As a result of the Data Breach, Plaintiff Blandford made reasonable efforts to mitigate the impact of the Data Breach, including checking his bills and accounts to make sure they were correct. Plaintiff Blandford has spent significant time dealing with the Data Breach, valuable time he 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.

153. As a result of the Data Breach, Plaintiff Blandford fears for his personal financial security and uncertainty over what medical information was revealed in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach and the resulting invasion of his privacy caused by the exposure of his private medical information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

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

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

156. Plaintiff Blandford has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Julie Hardin

157. Plaintiff Julie Hardin has, upon information and belief, worked trade shows for Defendant, and, in the course of her employment, provided her Private Information to Defendant.

158. Defendant obtained Plaintiff Hardin's Private Information in the course of conducting its regular business operations.

159. At the time of the Data Breach, Defendant maintained Plaintiff Hardin's Private Information in its system.

160. Plaintiff Hardin is very careful about sharing her sensitive Private Information. Plaintiff Hardin stores any documents containing their Private Information in a safe and secure

location. Plaintiff Hardin has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Hardin would not have entrusted their Private Information to Defendant had she known of Defendant's lax data security policies.

161. Plaintiff Hardin received a Notice Letter dated April 14, 2025, by U.S. mail, directly from Defendant, which informed Plaintiff Hardin that her Private Information was improperly accessed and obtained by unauthorized third parties, including her name, address, date of birth, Social Security Number, State identification number/Driver's License Number, Bank account information, and health information.[43]

162. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiffs to take other "precautionary measures…to protect your personal information" and to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis,"[44] Plaintiff Hardin made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the Data Breach. Plaintiff Hardin has spent significant time dealing with the Data Breach–valuable time she 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.

163. Plaintiff Hardin suffered actual injury from having her Private Information compromised as a result of the Data Breach, including, but not limited to: (i) invasion of privacy; (ii) theft of her 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

[43] *See* Exhibit A.
[44] For the Redacted Sample Notice Letter, *see* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mass.gov/doc/2025-681-nth-degree-investment-group/download

Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to her 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.

164. Plaintiff Hardin additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of their Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices by phishing attacks or elicit further personal information for use in committing identity theft or fraud.

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

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

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

168. Plaintiff Julie Hardin has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

169. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated, pursuant to GA Code § 9-11-23(a)-(c).

170. The Classes that Plaintiffs seek to represent are defined as follows:

Nationwide Class

> All individuals residing in the United States whose Private Information was accessed and/or acquired as a result of the Data Breach, including all people who were sent notice of the Data Breach.

California Subclass

> All individuals residing in California whose Private Information was accessed and/or acquired as a result of the Data Breach, including all people who were sent notice of the Data Breach.

171. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have 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 staff and immediate family members.

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

173. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of

individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted. The Classes are apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

174. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Among the questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, including the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members.

b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties.

c. Whether Defendant had respective duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes.

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members.

e. Whether and when Defendant actually learned of the Data Breach.

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised.

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised.

h. 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.

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur.

j. Whether Plaintiffs and Class Members are entitled to actual damages and/or nominal damages as a result of Defendant's wrongful conduct.

k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

175. Typicality: Plaintiffs' claims are typical of those of the other members of the Classes because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

176. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damage they have suffered are typical of other Class Members. Plaintiffs retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

177. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and

expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

178. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they 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 Plaintiffs was exposed is representative of that experienced by the Classes 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.

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

180. The litigation of the claims brought herein is manageable. Defendants' 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.

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

182. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

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

184. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiffs and the class of the Data Breach.

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information.

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts.

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence.

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

185. Plaintiffs re-allege and incorporate by reference all preceding allegations of paragraphs 1 through 184 of this Complaint, as if fully set forth herein.

186. Defendant requires its customers, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

187. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its customers and employees, which solicitations and services affect commerce.

188. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

189. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed.

190. By voluntarily undertaking and 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 common law duty of care to use reasonable means to secure and safeguard Class Members' Private Information, to prevent disclosure of the information, and to safeguard the information from theft.

191. Defendant's duty derived from common law, statutory law, and industry standards and included a responsibility to implement processes by which it could promptly detect a breach of its security systems, including adequate training or hiring of IT professional, stop a breach, and give prompt and complete notice to those affected by a data breach.

192. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statute was intended to guard against.

193. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

195. Defendant's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of being customers or employees of Defendant.

196. 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 Private Information.

197. Defendant was subject to the above "independent duties," untethered to any contract between Defendant and Plaintiffs or the Class.

198. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' and employees' Private Information it no longer needed to retain pursuant to regulations.

199. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

200. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

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

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

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

c. Allowing unauthorized access to Class Members' Private Information.

d. Failing to timely detect that Class Members' Private Information had been compromised by allowing the Data Breach to occur for *nine* days.

e. Failing to remove former customers' Private Information it no longer needed to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

202. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. 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 Plaintiffs and the Class. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

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

204. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and the known high frequency of cyberattacks and data breaches in the Global Marketing and Consumer solutions industry.

205. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information was wrongfully disclosed.

206. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures by Defendant, and Defendant knew or should have known of the inherent risks in collecting and storing the Private Information, the critical importance of providing adequate security of that Private Information, and the necessity of encrypting Private Information stored on Defendant's systems or transmitted through third-party systems.

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

208. Plaintiffs and the Class had no ability to protect their Private Information that was in, and, on belief, remains in, Defendant's possession.

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

210. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of the foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

211. Defendant has admitted that the Private Information of Plaintiffs and the Class was disclosed to unauthorized third persons as a result of the Data Breach.

212. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

214. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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.

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

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

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

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)

218. Plaintiffs re-allege and incorporate by reference the allegations of paragraphs 1 through 184 of this Complaint, as if fully set forth herein.

219. Section 5 of the Federal Trade Commission 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 companies, such as Defendant, of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

220. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct

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

221. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se.*

222. Class Members are consumers within the class of persons that Section 5 of the FTC Act was intended to protect.

223. Moreover, the harm that has occurred is the type of harm that the FTC Act 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 Plaintiffs and Class Members.

224. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

226. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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.

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

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

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

230. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

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

COUNT III
Breach Of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

232. Plaintiffs re-allege and incorporate by reference the allegations of paragraphs 1 through 184 of this Complaint, as if fully set forth herein.

233. Plaintiffs and Class Members were required to provide their Private Information to Defendant as part of the process of obtaining products or services provided by Defendant. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for products or services, and they would not have paid for Defendant's products or services, or would have paid less for them, had they known that Defendant's data security practices were substandard.

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

235. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

236. Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect their Private Information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

237. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

238. Implicit in the agreement between Plaintiffs and Class Members and the 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 Plaintiffs 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 Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

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

240. Defendant also promulgated, adopted, and implemented a written Privacy Policy, whereby it expressly promised Plaintiffs and Class Members that it was committed to protecting their Private Information and would only disclose the Private Information as authorized by law or contract. Plaintiff and Class Members fully performed their obligations under their contracts with Nth Degree, but Nth Degree did not secure or keep private Plaintiffs' and Class Members' Private Information, and therefore Nth Degree breached its contracts with Plaintiffs and Class Members.

241. On information and belief, Defendant further promised to comply with industry standards for protecting Plaintiffs' and Class Members' Private Information.

242. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant expend reasonable sums to obtain adequate data security. Defendant failed to do so.

243. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them that Defendant would keep their information reasonably secure.

244. Every contract has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

245. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

246. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide prompt and accurate notice of the Data Breach.

247. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information, and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

248. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, including, but not limited to: (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) lost opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (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.

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

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

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

251. Plaintiffs re-allege and incorporate by reference the allegations of paragraphs 1 through 184 of this Complaint, as if fully set forth herein.

252. Plaintiffs bring this Count in the alternative to the breach of implied contract count above.

253. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid Defendant and/or its agents for Global Marketing and event installation services and in so doing also provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

254. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

255. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

256. Defendant acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

257. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information at Defendant or obtained services at Defendant.

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

259. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

260. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon them.

261. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) 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) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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.

262. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

263. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
Declaratory Judgment
(On behalf of Plaintiffs and the Nationwide Class)

264. Plaintiffs re-allege and incorporate by reference the allegations of paragraphs 1 through 184 of this Complaint, as if fully set forth herein.

265. Under GA Code § 9-4-2 ("GA Declaratory Judgment Act"), this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal statutes described in this Complaint.

266. Nth Degree owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

267. Nth Degree still possesses Private Information regarding Plaintiff and Class Members.

268. Plaintiff alleges that Nth Degree's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Private Information and the risk remains that further compromises of his Private Information will occur in the future.

269. Under its authority pursuant to the GA Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Nth Degree owes a legal duty to secure its clients' Private Information and to timely notify its clients of a data breach under the common law, HIPAA, and Section 5 of the FTC Act;

b. Nth Degree's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect clients' Private Information; and

c. Nth Degree continues to breach this legal duty by failing to employ reasonable measures to secure its clients' Private Information.

270. This Court should also issue corresponding prospective injunctive relief requiring Nth Degree to employ adequate security protocols consistent with legal and industry standards to protect clients' Private Information, including the following:

a. Order Nth Degree to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Nth Degree must implement and maintain reasonable security measures, including, but not limited to:

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

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Nth Degree's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its users about the threats they face with regard to the security of their Private Information, as well as the steps Nth Degree's clients should take to protect themselves.

271. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Nth Degree. The risk of another such breach is real, immediate, and substantial. If another breach at Nth Degree occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

272. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Nth Degree if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Nth Degree's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Nth Degree has a pre-existing legal obligation to employ such measures.

273. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at

Nth Degree, thus preventing future injury to Plaintiffs and other clients whose Private Information would be further compromised.

COUNT VI
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On behalf of Plaintiff Blandford and the California Subclass)

274. Plaintiffs re-allege and incorporate by reference the allegations of paragraphs 1 through 184 of this Complaint, as if fully set forth herein.

275. Defendant violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to Plaintiff Blandford (for purposes of this section, the "Plaintiff") and the California Subclass (for purposes of this section, the "Class").

276. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class members' Private Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class members' Private Information in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods for safeguarding the Private Information of Plaintiff and the Class members.

277. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

278. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and Class members were injured and lost money or property, including but not limited to the price received by Defendant for the products and services, the loss of Plaintiff's and Class members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described herein.

279. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class members' Private Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class members.

280. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and Class members of money or property that Defendant may have acquired by means of its unlawful, and unfair business practices, disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VII
Violation of the California Consumer Records Act
Cal. Civ. Code § 1798.80, *et seq.*
(On Behalf of Plaintiff Blandford and the California Subclass)

281. Plaintiffs re-allege and incorporate by reference the allegations of paragraphs 1 through 184 of this Complaint, as if fully set forth herein.

282. Under the California Consumer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the

breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believes to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonable believes to have been, acquired by an unauthorized person." *Id.* (emphasis added).

283. The Data Breach constitutes a "breach of the security system" of Defendant.

284. An unauthorized person acquired the personal, unencrypted information of Plaintiff Blandford (for purposes of this section, the "Plaintiff") and the California Subclass (for purposes of this section, the "Class").

285. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff and the Class but waited four months to notify them after the Data Breach occurred. Given the severity of the Data Breach, this is an unreasonable delay.

286. Defendant's unreasonable delay prevented Plaintiff and the Class from taking appropriate measures to protect themselves against harm.

287. Because Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

288. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT VII
Violations of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798.150
(On behalf of Plaintiff Blandford and the California Subclass)

289. Plaintiffs re-allege and incorporate by reference the allegations of paragraphs 1 through 184 of this Complaint, as if fully set forth herein.

290. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Private Information of Plaintiff Blandford (for purposes of this section, the "Plaintiff") and the California Subclass (for purposes of this section, the "Class"). As a direct and proximate result, Plaintiff's and the Class members' nonencrypted and nonredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

291. Defendant is a "business" under the meaning of Civil Code § 1798.140 because Defendant is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civil Code § 1798.140(d).

292. Plaintiff and Class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Private Information, including Plaintiff's and the Class members' Private Information. Plaintiff and the Class members have an interest in ensuring that their Private Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

293. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and

Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

294. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

295. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

PRAYER FOR RELIEF

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and

assess whether monitoring tools are appropriately configured, tested, and updated;

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

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

xviii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

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

F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: December 19, 2025,

Respectfully Submitted,

/s/ Casondra Turner
Casondra Turner (GA Bar No. 418426)
MILBERG, PLLC
260 Peachtree Street NW, Suite 2200
Atlanta, GA 30303
Telephone: (866) 252-0878
Fax: (771) 772-3086
cturner@milberg.com

/s/ Andrew J. Shamis
Andrew J. Shamis
SHAMIS & GENTILE, P.A.
14 NE First Avenue, Suite 705
Miami, Florida 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com

Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: tbean@sirillp.com

Attorneys for Plaintiffs and the Proposed Class

**Pro hac vice application forthcoming*

EXHIBIT A

Nth Degree
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

PLP14500105673
JULIE M HARDIN
[redacted]

April 14, 2025

PLP14500105673056730102F0400

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear Julie M Hardin:

The privacy and security of the personal information we maintain is of the utmost importance to Nth Degree. We are writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently discovered that an unauthorized party gained access to our network environment.

What Are We Doing?

Upon learning of this issue, we immediately worked to contain the threat and secure our network environment. We commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal or sensitive data had been accessed or acquired as a result of this incident. After an extensive forensic investigation and manual document review, we discovered on March 24, 2025 that your personal information may have been accessed or acquired by an unauthorized party between on or around December 12, 2024 to on or around December 20, 2024.

What Information Was Involved?

The information potentially involved included your first and last name, address, date of birth, social security number, state identification number/driver's license number, bank account information, and health information.

What You Can Do?

We have no reason to believe that your information has been or will be used to commit financial fraud or identity theft as a result of this incident. Nevertheless, we are offering a complimentary twelve months membership of Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score through TransUnion. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. With this protection TransUnion will help you resolve issues if your identity is compromised.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, we recommend that you always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.