UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ALAN PITT, individually and on behalf of all others similarly situated, Plaintiff, v. **MADISON SQUARE GARDEN SPORTS CORP., MADISON SQUARE GARDEN ENTERTAINMENT CORP.** Defendant.	Case No. 26-5184 **CLASS ACTION COMPLAINT** **PROPOSED CLASS ACTION**

Plaintiff Alan Pitt, individually and on behalf of the Class defined below of similarly situated persons ("Plaintiff and Class Members"), alleges the following against Defendants, Madison Square Garden Sports Corp. (MSG Sports) and Madison Square Garden Entertainment Corp. (MSG Entertainment) (collectively, "Defendants"). The following allegations are based on Plaintiff's knowledge, investigations by Plaintiff's counsel, facts of public record, and information and belief:

NATURE OF THE ACTION

1. Plaintiff Seeks to hold Defendants responsible for the injuries that Defendants inflicted on Plaintiff and over 26 million others due to Defendants' egregiously inadequate data security, which resulted in the private information of Plaintiff and those similarly situated to be exposed to unauthorized third parties (the "Data Breach").

2. Defendant MSG Sports is located in New York, and is a leading professional sports company, with a collection of assets that includes the New York Knicks (NBA) and the New York Rangers (NHL), as well as two development league teams – the Westchester Knicks (NBAGL)

and the Hartford Wolf Pack (AHL).[1] MSG Sports also operates a professional sports team performance center – the MSG Training Center in Greenburgh, NY.[2]

3. Defendant MSG Entertainment is a leader in live entertainment and its portfolio includes a collection of world-renowned venues – New York's Madison Square Garden, Infosys Theater at Madison Square Garden, Radio City Music Hall, and Beacon Theatre; and The Chicago Theatre – that showcase a broad array of sporting events, concerts, family shows, and special events for millions of guests annually.[3] In addition, the Company features the original production, the *Christmas Spectacular Starring the Radio City Rockettes*, which has been a holiday tradition for more than 90 years. More information is available at www.msgentertainment.com. New York's Madison Square Garden is widely known as the "coolest Arena" in the United States by *Rolling Stone* and "Venue of the Decade" by *Billboard*.[4] It has been around since 1879 and has been a celebrated center of New York life, epitomizing the experience of live sports and entertainment to people.[5]

4. The data that Defendants exposed to the public is unique and highly sensitive. For one, the exposed data included personal identifying information ("PII") allegedly including files mentioning specific sports teams, and specifically Knicks-related personalities, with fields such as

[1] Madison Square Garden Sports Corp. Reports, Fiscal 2026 Third Quarter Results, https://www.sec.gov/Archives/edgar/data/1636519/000162828026032551/msgsportscorpex991forearni.htm (last accessed on June 17, 2026).
[2] *Id.*
[3] Madison Square Garden Entertainment Corp. Reports, Fiscal 2026 Third Quarter Results, https://www.sec.gov/Archives/edgar/data/1952073/000162828026031682/msgeex99133126.htm (last accessed on June 17, 2026).
[4] History of Madison Square Garden, https://www.msg.com/madison-square-garden/history (last accessed on June 17, 2026).
[5] *Id.*

"address," "claim to fame," "cost of talent," and sometimes contact information for them or their representatives (collectively "Private Information").[6]

5. Plaintiff and Class Members provided this information to Defendants with the understanding that Defendants would keep that information private in accordance with both state and federal laws.

6. Defendants have yet to announce the Data Breach to the public, exacerbating the anxiety of the Plaintiff and Class Members and depriving them of the chance to take speedy measures to protect themselves and mitigate harm.

7. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. Defendants' woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

8. Today, the Private Information of Plaintiff and Class Members continues to be in jeopardy because of Defendant's actions and inactions described herein. Plaintiff and Class Members now suffer from a heightened and imminent risk of fraud and identity theft for years to come and now must constantly monitor their medical and financial accounts for unauthorized activity.

9. The Private Information exposed in the Data Breach can enable criminals to commit a litany of crimes. Criminals can open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' Private Information to craft phishing and other hacking attacks based on Class

[6] Hackers Publish Knicks and Madison Square Garden Data Online, https://www.404media.co/hackers-publish-knicks-and-madison-square-garden-data-online/ (last accessed on June 17, 2026).

Members' individual needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

10. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) anxiety, annoyance, and nuisance; (k) continued risk to their Private Information, which remains in Defendants' possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information; and (l) disgorgement damages associated with Defendants' maintenance and use of Plaintiff's and Class Members' data for its benefit and profit.

11. Through this action, Plaintiff seeks to remedy these injuries on behalf of Himself and all similarly situated individuals whose Private Information was exposed and compromised in the Data Breach.

12. Plaintiff brings this action against Defendants and asserts claims for negligence, negligence *per se*, unjust enrichment, breach of fiduciary duty, and breach of implied contract.

PARTIES

13. Plaintiff Alan Pitt is a natural person, resident, and citizen of Atlanta, Georgia.

14. Defendant Madison Square Garden Sports Corp. is a Nevada corporation with its principal place of business located at Two Pennsylvania Plaza, New York, NY, United States, 10121.

15. Defendant Madison Square Garden Entertainment Corp. is a Nevada corporation with its principal place of business located at Two Pennsylvania Plaza, New York, NY, United States, 10121.

JURISDICTION AND VENUE

16. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because members of the Nationwide Class are citizens of states different than Defendants.

17. This Court has general personal jurisdiction over Defendants because Defendants' principal place of business is in New York. Defendants also regularly conduct substantial business in New York.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendants conduct substantial business in this District.

FACTUAL ALLEGATIONS

Defendants Collected and Stored the Private Information of Plaintiff and Class Members

19. Defendant MSG Sports is located in New York, and is a leading professional sports company, with a collection of assets that includes the New York Knicks (NBA) and the New York

Rangers (NHL), as well as two development league teams – the Westchester Knicks (NBAGL) and the Hartford Wolf Pack (AHL).[7] MSG Sports also operates a professional sports team performance center – the MSG Training Center in Greenburgh, NY.[8]

20. Defendant MSG Entertainment is a leader in live entertainment and its portfolio includes a collection of world-renowned venues – New York's Madison Square Garden, Infosys Theater at Madison Square Garden, Radio City Music Hall, and Beacon Theatre; and The Chicago Theatre – that showcase a broad array of sporting events, concerts, family shows, and special events for millions of guests annually.[9] In addition, the Company features the original production, the *Christmas Spectacular Starring the Radio City Rockettes*, which has been a holiday tradition for more than 90 years. More information is available at www.msgentertainment.com. New York's Madison Square Garden is widely known as the "coolest Arena" in the United States by *Rolling Stone* and "Venue of the Decade" by *Billboard*.[10] It has been around since 1879 and has been a celebrated center of New York life, epitomizing the experience of live sports and entertainment to people.[11]

21. Plaintiff and Class Members provided their Private Information to Defendants as a requirement to obtain services from Defendants.

22. Defendants collect Private Information from Plaintiff and Class Members in the ordinary course of business along with facial recognition and biometric data, through their

[7] Madison Square Garden Sports Corp. Reports, Fiscal 2026 Third Quarter Results, https://www.sec.gov/Archives/edgar/data/1636519/000162828026032551/msgsportscorpex991forearni.htm (last accessed on June 17, 2026).
[8] *Id.*
[9] Madison Square Garden Entertainment Corp. Reports, Fiscal 2026 Third Quarter Results, https://www.sec.gov/Archives/edgar/data/1952073/000162828026031682/msgeex99133126.htm (last accessed on June 17, 2026).
[10] History of Madison Square Garden, https://www.msg.com/madison-square-garden/history (last accessed on June 17, 2026).
[11] *Id.*

sprawling surveillance that is collects for personal gain. Upon information and belief, this Private Information is then stored on Defendants' systems or systems that Defendants controls.

23. Because of the highly sensitive and personal nature of the information Defendants acquire and store, Defendants knew or reasonably should have known that they must comply with industry standards related to data security and all federal and state laws protecting Private Information and provide adequate notice if Private Information is disclosed without proper authorization.

24. Plaintiff and Class Members provided their Private Information to Defendants as a condition of receiving services from Defendants, but in doing so, expected Defendants to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

25. Upon information and belief, Plaintiff's and Class Members' affected Private Information at the time of the Data Breach was accessible, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals. Upon information and belief, the affected Private Information was not encrypted.

26. Upon information and belief, Defendants were a target due to their status as entities that collect, create, and maintain Private Information.

27. Upon information and belief, the threat group ShinyHunters claimed responsibility for the attack.[12] The group claimed that the breach affected more than 42 GB of uncompressed/internal files and confidential information, including over 26 million records.[13]

[12] Hackers Publish Knicks and Madison Square Garden Data Online, https://www.404media.co/hackers-publish-knicks-and-madison-square-garden-data-online/ (last accessed on June 17, 2026).
[13] *Id.*

28. Among the more notable details in the Private Information are records that appear to go beyond basic contact information and operational data.[14] Files reportedly included internal risk designations, talent valuations, and other information tied to how the organization tracked and managed relationships with prominent individuals.[15]

29. Defendants have yet to announce the Data Breach to the public, exacerbating the anxiety of the Plaintiff and Class Members and depriving them of the chance to take speedy measures to protect themselves and mitigate harm, leaving them wondering how they can protect themselves.

30. Time is of the essence when highly sensitive Private Information is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired Private Information of Plaintiff and Class Members is now likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Private Information to criminals.

31. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Private Information, onto the Dark Web. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive information.

32. Defendants largely put the burden on Plaintiff and Class Members to take measures to protect themselves from identity theft and fraud.

[14] ShinyHunters Exposes Massive MSG Data and Internal Risk Ratings, The National CIO Review, https://nationalcioreview.com/articles-insights/extra-bytes/shinyhunters-exposes-massive-msg-data-and-internal-risk-ratings/ (last accessed on June 17, 2026).
[15] *Id.*

33. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protection services for their respective lifetimes.

34. Plaintiff and the Class Members remain in the dark regarding exactly what data was stolen, the particular method of disclosure, the results of any investigations, and what steps are being taken, if any, to secure their Private Information going forward. They are further left to speculate as to the full impact of the Data Breach and how exactly Defendants intend to enhance their information security systems and monitoring capabilities so as to prevent further breaches.

35. Defendants could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting their servers and systems, generally, as well as the Private Information that they chose to store.

36. Defendants' negligence in safeguarding that Private Information was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

37. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.4% are salaried.[16]

38. According to the American Time Use Survey, American adults have between 4 to 6 hours of "leisure time" outside of work per day;[17] examples of leisure time include partaking in sports, exercise and recreation; socializing and communicating; watching TV; reading;

[16] *Characteristics of minimum wage workers, 2022*, U.S. Bureau of Labor Statistics (Aug. 2023), https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm (last accessed on Aug. 6, 2024).
[17] *Americans have no idea how to use their free time*, Business Insider (Mar. 26, 2024), https://www.businessinsider.com/americans-free-time-leisure-dont-use-television-2024-3 (last accessed on Aug. 6, 2024).

thinking/relaxing; playing games and computer use for leisure; and other leisure activities.[18] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

39. Plaintiff and Class Members are deprived of the choice as to how to spend their valuable free hours and therefore seek remuneration for the loss of valuable time as another element of damages.

Defendants Failed to Comply with FTC Guidelines

40. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[19] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of Private Information.

41. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[20] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

---

[18] *Table 11A. Time spent in leisure and sports activities for the civilian population by selected characteristics, averages per day, 2022 annual averages*, U.S. Bureau of Labor Statistics (June 22, 2023), https://www.bls.gov/news.release/atus.t11A.htm (last accessed on Aug. 6, 2024).

[19] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf. (last accessed on Aug. 6, 2024).

[20] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed on Aug. 6, 2024).

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

42. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

43. The FTC 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.[21]

44. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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.

45. These FTC enforcement actions include actions against providers and partners like Defendants. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

[21] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf (last accessed on Aug. 6, 2024).

46. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

47. Despite their alleged commitments to securing sensitive data, Defendants do not follow industry standard practices in securing Private Information.

48. As shown above, experts studying cyber security routinely identify entities storing vast amounts of sensitive information like Social Security numbers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

49. Several best practices have been identified that at a minimum should be implemented by entities like Defendants, including but not limited to, educating all employees on the risks of cyber attacks; 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.

50. Other best cybersecurity practices that are standard in such industries 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.

51. Upon information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-

2), and the Center for Internet Security's Critical Security Controls ("CIS CSC"), which are all established standards in reasonable cybersecurity readiness.

52. Such frameworks are the existing and applicable industry standards. Defendants failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

Plaintiff Alan Pitt's Experiences and Injuries Caused by the Data Breach

53. As a prerequisite of being able to obtain services from Defendants, Defendants required individuals to provide their Private Information.

54. Defendants have yet to notify Plaintiff and Class Members of the Data Breach.

55. Because of the Data Breach, Defendants inflicted injuries upon Plaintiff and Class Members. And yet, Defendants have done little to provide them with relief for the damages they suffered.

56. Defendants obtained Plaintiff's information as a prerequisite for Plaintiff to obtain services from Defendants. Defendants collect and maintain personal and sensitive information of its customers, such as Plaintiff, presumably to provide its services.

57. Plaintiff attended three events at the Beacon Theatre in 2025 and has attended many events at the Sphere. Defendants collected and, upon information and belief, maintain personal and sensitive information of Plaintiff from each of these events.

58. Plaintiff hasn't received from Defendant a notice of the Data Breach.

59. Plaintiff is a reasonably cautious person and is therefore careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing Personal Information in a safe and secure location or destroys the

documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for various online accounts, changing and refreshing them as needed to ensure Private Information is as protected as it can be. When it is available, Plaintiff uses two-factor or multifactor authentication to add an extra layer of security.

60. Plaintiff only allowed Defendants to maintain, store, and use his Private Information because of the belief that Defendants would use security measures to protect that Private Information, such as requiring passwords and multi-factor authentication to access databases storing that Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendants at the time of the Data Breach.

61. In the instant that Plaintiff's Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

62. Plaintiff has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that was entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

63. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

64. The substantial risk of imminent harm and loss of privacy has caused Plaintiff to suffer stress, fear, and anxiety. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff and the Class Face Significant Risk of Present and Continuing Identity Theft

65. Plaintiff and Class Members suffered injury from the misuse of their Private Information that can be directly traced to Defendants.

66. The ramifications of Defendants' failure to keep Plaintiff's and the Class Members' Private Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

67. In 2021, 32% of persons aged 16 or older who received breach notification were victims of multiple types of identity theft.[22]

68. As a result of Defendants' failures to prevent the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future

[22] Erika Harrell, PhD, *Data Breach Notifications and Identity Theft, 2021*, U.S. Bureau of Justice Statistics (Jan. 2024), https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021. (last accessed on Aug. 6, 2024).

consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in their possession.

69. Stolen PII and PHI (like the Private Information at issue here) is one of the most valuable commodities on the criminal information black market. According to Prey, a company that develops device tracking and recovery software, stolen PII and PHI (like the Private Information at issue here) can be worth up to $2,000.00 depending on the type of information obtained.[23]

70. The value of Plaintiff's and Class Members' Private Information on the black market is considerable. Stolen information (similar if not identical to the Private Information at issue in this litigation) trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

71. It can take victims years to spot or identify theft, giving criminals plenty of time to milk that information for cash.

[23] Juan Hernandez, *The Lifecycle of Stolen Credentials on the Dark Web*, Prey (Feb. 26, 2024), https://preyproject.com/blog/lifecycle-stolen-credentials-dark-web (last accessed on Aug. 6, 2024).

72. One such example of criminals using PII and/or PHI (like the Private Information at issue here) for profit is the development of "Fullz" packages.[24]

73. Cyber-criminals can cross-reference two sources of PII and/or PHI (like the Private Information at issue here) 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. These dossiers are known as "Fullz" packages.

74. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff 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 stolen by the cyber-criminals in the Data Breach, criminals can 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. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

[24] "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 can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SEC. (Sep. 18, 2014), https://krebsonsecurity.com/tag/fullz/ (last accessed on Aug. 6, 2024).

75. According to the FBI's Internet Crime Complaint Center (IC3) 2023 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $12.5 billion in losses to individuals and business victims.[25]

76. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

77. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

78. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[26]

79. The FTC has issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data

[25] *2023 Internet Crime Report*, Fed. Bureau of Investig. (2023), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (last accessed on Aug. 6, 2024).
[26] *Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last accessed on Aug. 6, 2024).

security into all business decision-making.[27] According to the FTC, data security requires: (1) controlling access to data sensibly; (2) requiring secure passwords and authentication; (3) storing sensitive information securely and protecting it during transmission; (4) segmenting networks and monitoring who is trying to get in and out; (5) securing remote access to networks; (6) applying sound security practices when developing new products; (7) ensuring that third-party service providers implement reasonable security measures; (8) putting in place procedures to keep security current and address potential vulnerabilities; and (9) securing paper, physical media, and devices.[28]

80. According to the FTC, unauthorized PII and PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[29] The FTC treats 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(a) of the FTCA.

81. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-

[27] *Start With Security, A Guide for Business*, Fed. Trade Comm'n (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf. (last accessed on Aug. 6, 2024).
[28] *Id*.
[29] *See Taking Charge, What to Do If Your Identity is Stolen*, FED. TRADE COMM'N, at 3 (Jan. 2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last accessed on Aug. 26, 2024).

4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of Private Information.

82. Charged with handling highly sensitive Private Information including facial recognition and biometric data through their sprawling surveillance machines, Defendants knew or should have known the importance of safeguarding the Private Information that was entrusted to them Because they failed to do so, tens of millions of individuals are at increased risk of identity theft, fraud, and other crime.

83. Defendants also knew or should have known of the foreseeable consequences if its data security systems were breached, given their collection of highly sensitive Personal Information, they were at an increased risk of cyberattacks. Defendants nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

84. Defendants' use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology

security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the Plaintiff's and Class Members' Private Information to unscrupulous operators, con artists, and outright criminals.

CLASS ACTION ALLEGATIONS

85. Plaintiff brings this class action individually and on behalf of all similarly situated persons under Federal Rule of Civil Procedure 23. Plaintiff seeks certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3), and (c)(4) of the following Nationwide Class (the "Class"):

> All persons in the United States whose Private Information was accessed in the Defendant's Data Breach.

86. The Class defined above is readily ascertainable from information in Defendants' possession. Thus, such identification of Class Members will be reliable and administratively feasible.

87. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendants or their parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

88. Plaintiff reserves the right to amend or modify the Class definitions as this case progresses.

89. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

90. **Numerosity**. Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown at this time, based on information and belief, the Class consists of the approximately 26 million individuals whose Private Information was accessed and compromised by Defendants' Data Breach.

91. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Plaintiff and Class Members alike to safeguard their Private Information;

f. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

g. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

h. Whether Defendants should have discovered the Data Breach and reported it;

i. Whether Defendants' delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

j. Whether Defendants' conduct was negligent;

k. Whether Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

l. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

m. Whether an implied contract existed between Plaintiff and Class Members;

n. Whether Defendants breached implied contracts with Plaintiff and Class Members;

o. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred by Plaintiff and Class Members;

p. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;

q. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

92. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was accessed and compromised in the Data Breach. Moreover, Plaintiff and Class Members were subjected to Defendants' uniformly illegal and impermissible conduct.

93. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

94. **Predominance**. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' Private Information was stored on the same computer system and unlawfully exposed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

95. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

96. 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.

97. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

98. Likewise, particular issues under Federal Rule of Civil Procedure 23(c)(4) 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 those set forth above.

99. Defendants have 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.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

100. Plaintiff alleges and incorporates by reference paragraphs 1 to 97 of the Complaint as if fully set forth herein.

101. Defendants required Plaintiff and Class Members to provide Defendants with their Private Information in order to receive Defendants' products and services.

102. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard its computer system—and Plaintiff's and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes so they

could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

103. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendants hold vast amounts of sensitive information, it was inevitable that unauthorized individuals would at some point try to access Defendants' databases that store that sensitive information, including the Private Information at issue in this litigation.

104. After all, Private Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing Plaintiff's and Class Members' Private Information. Thus, Defendants knew, or should have known, the importance of exercising reasonable care in handling the Private Information entrusted to it.

105. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

106. Defendants' duty of care to use reasonable security measures arose because of the special relationship that existed between Defendants on the one hand, and Plaintiff and Class Members on the other hand, recognized by common law and existing regulations. Defendants were in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

107. Defendants failed to take appropriate measures to protect Plaintiff's and the Class Members' Private Information. Defendants are morally culpable, given the prominence of security

breaches in this industry. Any purported safeguards that Defendants had in place were wholly inadequate, as demonstrated by the Data Breach.

108. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in this industry, and allowing unauthorized access to Plaintiff's and Class Members' Private Information.

109. The failure of Defendants to comply with industry and regulations evinces Defendants' negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

110. But for Defendants' wrongful and negligent breach of their duties to Plaintiff and the Class, Private Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of Plaintiff's and Class Members' Private Information and all resulting damages.

111. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information. Defendants knew or should have known that its systems and technologies for processing and securing the Plaintiff's and Class Members' Private Information had security vulnerabilities.

112. As a result of this misconduct by Defendants, the Private Information and other sensitive information belonging to Plaintiff and Class Members was compromised, placing them at a greater risk of identity theft and their Private Information being disclosed to third parties without the consent of Plaintiff and Class Members.

113. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; (vi) 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives; (viii) the present value of ongoing credit monitoring and identity defense services necessitated by Defendants' data breach; (ix) the value of the unauthorized access to their Private Information permitted by Defendant; and (x) any nominal damages that may be awarded.

114. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members 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 including nominal damages.

115. Defendants' negligent conduct is ongoing, in that it still possesses the Private Information in an unsafe and insecure manner.

116. As a direct and proximate result of Defendants; negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Class)

117. Plaintiff alleges and incorporates by reference paragraphs 1 to 97 of the Complaint as if fully set forth herein.

118. Defendants had duties arising under the FTCA to protect Plaintiff's and Class Members' Private Information.

119. Defendants breached their duties, pursuant to the FTCA and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized access to Class Members' Private Information; (iv) failing to detect in a timely manner that Class Members' Private Information had been compromised; (v) failing to remove Private Information it was no longer required to retain pursuant to regulations; and (vi) 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.

120. Defendants' violation of Section 5 of the FTCA (and similar state statutes) constitutes negligence *per se*.

121. Plaintiff and Class Members are consumers within the class of persons that Section 5 of the FTCA was intended to protect.

122. The harm that has occurred is the type of harm the FTCA was intended to guard against.

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

124. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

125. Plaintiff and Class Members were foreseeable victims of Defendants' violations of the FTCA. Defendants knew or should have known that their failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class.

126. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

127. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members 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.

128. Finally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

129. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

130. Plaintiff alleges and incorporates by reference paragraphs 1 to 97 of the Complaint as if fully set forth herein.

131. Plaintiff and Class Members conferred a benefit on Defendants by entrusting their Private Information to Defendant from which Defendants derived profits.

132. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members,

on the other hand, suffered as a direct and proximate result of Defendants' failure to provide adequate security.

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

134. Defendants acquired the Private Information at issue in this litigation through inequitable means in that Defendants failed to disclose the inadequate security practices and failed to maintain adequate data security.

135. If Plaintiff and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to disclose their Private Information to Defendants.

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

137. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; (vi) 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 Defendants' possession and is subject to further unauthorized disclosures or further entrustment to inadequate third party vendors so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable

and continuing consequences of compromised Private Information for the rest of their lives; (viii) the present value of ongoing credit monitoring and identity defense services necessitated by Defendants' data breach; (ix) the value of the unauthorized access to their Private Information permitted by Defendants; and (x) any nominal damages that may be awarded.

138. Plaintiff and Class Members are entitled to restitution and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct, as well as return of their sensitive Private Information and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

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

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Nationwide Class)

140. Plaintiff alleges and incorporates by reference paragraphs 1 to 97 of the Complaint as if fully set forth herein.

141. A relationship existed between Plaintiff and Class Members on the one hand, and Defendants on the other, which arose from: (a) Defendants' acceptance of Plaintiff's and Class Members' Private Information; and (b) Defendants' representations of their commitment to protect said Private Information.

142. Defendants became the guardian of Plaintiff's and Class Members' Private Information. Defendants became a fiduciary, created by their undertaking and guardianship of Plaintiff's and Class Members' Private Information, to act primarily for their benefit. This duty

included the obligation to safeguard Plaintiff's and Class Members' Private Information and to timely detect and notify Plaintiff and Class Members in the event of a data breach.

143. The interests of public policy mandates that a fiduciary duty is imputed given Defendants' acceptance of Plaintiff's and the Class Members' Private Information and Defendants' representations of its commitment to protect said Private Information.

144. Defendants breached the fiduciary duty that they owed to Plaintiff and Class Members because Defendants failed to act with the utmost good faith, fairness, honesty, the highest degree of loyalty, ultimately failed to protect that Private Information.

145. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiff and Class Members.

146. But for Defendants' breach of fiduciary duty, the damage to Plaintiff and Class Members would not have occurred.

147. Defendants' breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class Members.

148. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff and Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their Private Information is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how

to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession and ensure that they retain vendors who adequately protect Private Information; (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of the Private Information compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (h) nominal damages.

149. As a direct and proximate result of Defendants' breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

150. Plaintiff alleges and incorporates by reference paragraphs 1 to 97 of the Complaint as if fully set forth herein.

151. Through their course of conduct, Defendants on the one hand, and Plaintiff and Class Members on the other, entered into implied contracts for Defendants to implement data security adequate to safeguard Plaintiff's and Class Members' Private Information.

152. Specifically, Plaintiff and Class Members entered into a valid and enforceable implied contract with Defendants when they availed Defendants' services.

153. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendants include the promise to protect non-public Private Information given to Defendants or that Defendants create on their own from disclosure.

154. When Plaintiff and Class Members provided their Private Information to Defendants, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

155. Defendants and/or their agents solicited and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

156. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, and were consistent with industry standards.

157. Class Members who paid money to Defendants reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

158. Implicit in the implied contracts, Defendants promised and were obligated to: (a) take reasonable steps to safeguard that Private Information, including through proper vetting of third party vendors to whom Private Information is provided; (b) prevent unauthorized disclosure of the Private Information; (c) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; (d) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses; and (e) retain or allow third parties to retain Private Information only under conditions that kept such information secure and confidential.

159. In accepting the Private Information, Defendants understood and agreed that they were required to reasonably safeguard and otherwise ensure protection of the Private Information from unauthorized access or disclosure.

160. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract requiring Defendants to keep their Private Information secure.

161. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied promise to monitor and ensure that the Private Information entrusted to them would remain protected by reasonable data security measures and remain confidential, either in the hands of Defendants or anyone under Defendants' control or agency.

162. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants by providing their Private Information at Defendants' request.

163. Defendants materially breached their contractual obligation to protect the non-public Private Information Defendants gathered when the sensitive information was accessed by unauthorized persons during and after the Data Breach.

164. Defendants materially breached the terms of the implied contracts. Defendants did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by the Data Breach. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

165. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

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

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

168. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, at minimum (and to be expanded following discovery): (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit and identity monitoring to all Class Members.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, on behalf of himself and all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class Representative;

B. A mandatory injunction directing Defendants to adequately safeguard Plaintiff's and Class Members' Private Information by implementing improved security procedures and measures, including but not limited to an Order:

   i. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

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

iii. Requiring Defendants to delete and purge Plaintiff's and Class Members' Private Information unless Defendants can justify reasonable bases for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private Information;

v. Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

vi. Prohibiting Defendants from maintaining Plaintiff's and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

vii. Requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

viii. Requiring Defendants to conduct regular database scanning and securing checks;

ix. Requiring Defendants to monitor ingress and egress of all network traffic;

x. Requiring Defendants 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 Private Information, and protecting the Plaintiff's and Class Members' Private Information;

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

xii. Requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendants' networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. Requiring Defendants to meaningfully educate all Class Members about the threats that they face because of the loss of that confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendants provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons;

D. A mandatory injunction requiring Defendants to purchase credit monitoring and identity theft protection services for each Class Member for life;

E. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

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

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and any other interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: June 18, 2026

Respectfully Submitted,

/s/ Jonathan Sedgh

JONATHAN SEDGH
jsedgh@forthepeople.com
MORGAN & MORGAN
199 Water St, Suite 1500,
New York, NY
Phone: (212) 738-6839
Fax: (718) 510-9352

JOHN A. YANCHUNIS*
jyanchunis@forthepeople.com
RIYA SHARMA*
rsharma@forthepeople.com
JAYDEN MOUGIN*
Jayden.mougin@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Phone: (813) 275-5272
Fax: (813) 222-4736

*****Pro hac vice forthcoming.*

Counsel for Plaintiff and the Class