UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CARLOS AVALOS, on behalf of himself and all others similarly situated, *Plaintiff*, v. MADISON SQUARE GARDEN ENTERTAINMENT CORPORATION, *Defendant.*	Case No. _____ CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff CARLOS AVALOS ("Plaintiff"), on behalf of himself and all others similarly situated, brings this Class Action Complaint against Defendant MADISON SQUARE GARDEN CORPORATION ("MSG" or the "Defendant"), for violations of state and common laws set forth herein in connection with Defendant's failures to allow for the unlawful breach of personally identifiable and sensitive information during the applicable statutory period and continuing through the present day ("Class Period").

Plaintiff makes the following allegations based upon personal knowledge as to himself, extensive investigative and media reporting, dark web postings from the perpetrators, alerts from various data security infrastructures, as well as upon information and the belief and investigation of his counsel as follows:

SUMMARY OF THE CASE

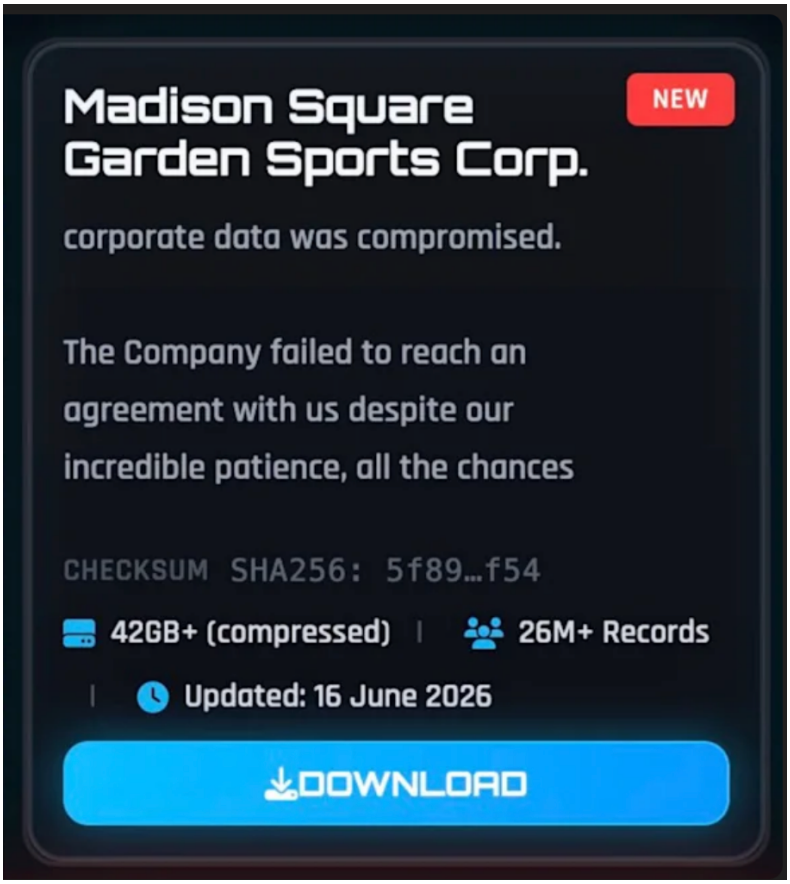
1. This is an Action against Defendant MSG for their recidivist disregard for consumer privacy and MSG's complete and utter failure to properly secure and safeguard personally identifiable information ("PII") including but not limited to the information of up to 26 million consumers, including Plaintiff's and Class members' personal information (the "Data Breach").

2. Madison Square Garden, which is owned by the Defendant as well as its famous tenants (the NBA champion New York Knicks and the New York Rangers), is well regarded as one of the world's most famous sports arenas. The arena is the sole professional sports venue located within Manhattan in New York City – and attracts visitors from around the world (the "Arena").

3. Unfortunately, Defendant has a tempestuous history with respect to data privacy. Defendant is infamous for collecting biometric facial recognition data from each consumer which enters into the Arena. Despite a slew of lawsuits regarding this conduct, as well as consternation from privacy advocates and legislators in New York, the Arena – at the direction of its owner James Dolan – continues to collect biometric information from each visitor. The reason for this is to use biometric data and combine it with other characteristic information and social media posting to create threat assessment profiles on each entrant into the Arena, which, upon information and belief, may have been compromised in this Data Breach.

4. Additionally, this is not MSG's first major data breach, including a point-of-sale attack which compromised payment card for visitors to the Arena 2015-2016 and a more recent data breach from 2025 by the notorious hacking/cybercriminal organization Cl0p which exploited an Oracle Business Suite vulnerability to expose tens of thousands of names and Social Security numbers for former and current employees. And yet, Defendant continued to collect, retain, and otherwise use the personal information of consumers to create threat assessments and for other purposes despite showing it was clearly incapable of handling this sensitive data.

5. On June 16, 2026, the notorious cybercriminal organization called ShinyHunters announced their infiltration into MSG's computer networks – stating, we have "*It's very simple. When you pay us, your data is deleted, and you move on with your life. When you don't pay us, you get posted here, among other things.*" That same day, the following publication appeared on ShinyHunters' Data Leak Site ("DLS") which contains over 42 GB of compressed data and over 26 million consumer records:



6. Defendant purportedly had a substantial amount of time to pay a ransom – which means that ShinyHunters was able to penetrate Defendant's unmonitored system and likely lock it down until a sum was paid in exchange for the PII which would eventually be leaked in the Data Breach. ShinyHunters also set a deadline of June 15, 2026 to inform the cybercriminal organization of whether or not the ransom would be paid: which it likely was not given the Data Breach. This also means Defendant had notice of the Data Breach for some time, and opted not to inform consumers of the risk of their data being exposed.

7. While the corpus of the PII remains unclear, what is clear is that the data exposed includes over 26 million lines of consumer information – and that a profile of two consumers, who happen to be celebrities, was presented by ShinyHunters to media sources who confirmed that the profiles were risk assessments which have been detailed as being tied to biometric facial

recognition profiles combined with the consumer's name and other sensitive demographic and characteristic information which allowed Defendant to assign a risk assessment to each individual which enters into the Arena.

8. Plaintiff brings this Action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) protect the PII of Plaintiff and Class members; (ii) warn Plaintiff and Class members of Defendant's inadequate information security; (iii) effectively secure the hardware containing the protected PII using reasonable and adequate safeguards free of vulnerabilities; and (iv) provide timely notice to the many victims of the Data Breach.

9. As such, Plaintiff brings this Action on behalf of himself and all others similarly situated for negligence and negligence *per se* seeking actual and punitive damages, as well as attorneys' fees, costs, and expenses, along with appropriate injunctive and declaratory relief.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount of controversy exceeds the sum of $5,000,000 exclusive of interests and costs, there are more than 100 putative Class members, and minimal diversity exists because one or more putative Class members are citizens of a different state than a Defendant. On an annual basis, over four million visitors attend concerts and sporting events at the arena – and the corpus of data purportedly includes over 26 million profiles.

11. This Court has personal jurisdiction over MSG because MSG maintains its principal place of business in New York, New York. Furthermore, MSG intentionally availed itself of this jurisdiction by marketing, employing individuals, and providing services in New York and MSG maintains significant contacts, including millions of New Yorkers, who were impacted by the Data Breach.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because MSG operates in this District and a substantial part of the events, acts and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

PLAINTIFF

Plaintiff Carlos Avalos

13. Plaintiff Carlos Avalos is, and at all times mentioned herein, was an individual citizen of the state of New York.

14. Plaintiff's PII was collected by Defendant while attending a concert at the Arena in September of 2025. Plaintiff reasonably believes that his PII was compromised in the Data Breach given that the threat assessment profiles of over 26 million visitors to the Arena were exposed, including the profiles of guests (included in the sample presented to the media) who attended events at the Arena within the same calendar year as Plaintiff's visit to the Arena.

15. Plaintiff is gravely concerned about the sensitive information that was exposed in the Data Breach, and now has time trying to ascertain whether and how to protect his PII and monitoring for phishing attacks and other types of intrusive, interruptive repercussions of the Data Breach

DEFENDANT

Defendant Madison Square Garden Entertainment Corporation

16. Defendant Madison Square Garden Entertainment Corporation is a Nevada corporation with its principal place of business located in New York, New York at Two Pennsylvania Plaza, New York, New York 10121.

17. Defendant owns the Arena, as well as the New York Knicks, the New York Rangers, the Sphere (located in Las Vegas, Nevada), Radio City Music Hall, the Chicago Theatre, the Beacon Theatre, and other entertainment and dining entities.

FACTUAL ALLEGATIONS

Defendant's Businesses and Collection of Private Information

18. In the course of doing business, Defendant collects a significant amount of highly valuable private information from guests to the Arena as well as its employees who work at the Arena, including the collection of the PII of Plaintiff and the Class members.

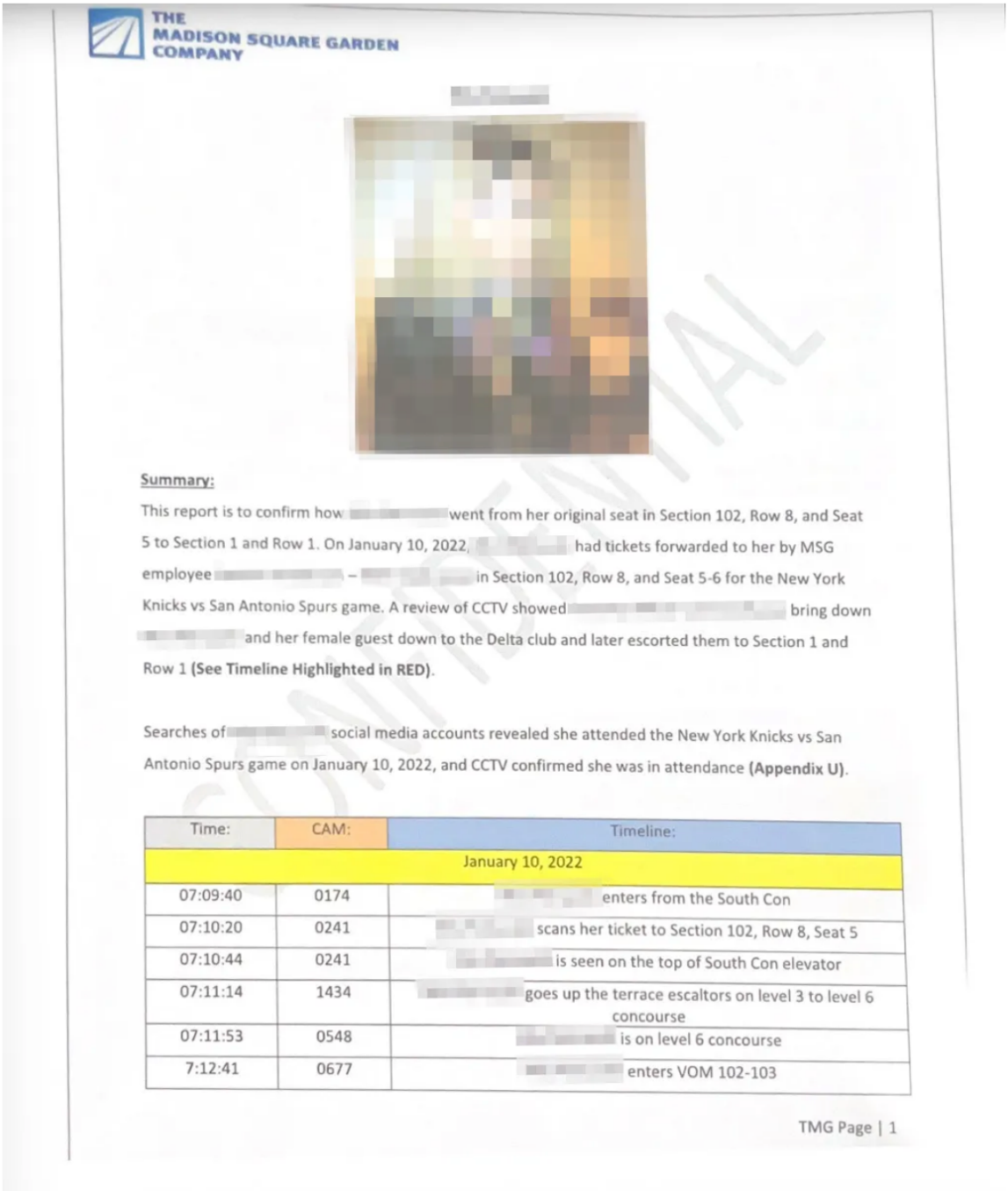
19. According to reports, Defendant implemented a facial recognition system beginning in 2018 but has engaged in various types of mass surveillance of visitors to the Arena and of the surrounding neighborhood including using members of Defendant's security disguised as police officers to spy on local protesters.[1] Defendant's security apparatus knows no bounds, compiling dossiers on individuals and screen-grabbing the law firm photos of over 1,200 lawyers who presented "threats" to Defendant by way of litigating cases against it – including the undersigned counsel – to feed them into the Arena's facial recognition and surveillance system to ban from the Arena.

20. The facial recognition system is also used to identify visitors from the second they enter the Arena, which is publicly known.[2] Defendant's facial recognition system and technology surveillance system within the Arena allows Defendant to track visitors on a second-by-second

[1] Bobby Silverman and Noah Schactman, "*Inside Madison Square Garden's Surveillance Machine*," WIRED (ONLINE) (Apr. 23, 2026), at https://www.wired.com/video/watch/how-we-exposed-the-shocking-secrets-of-madison-square-gardens-surveillance-machine-and-why-it-matters-to-everyone.

[2] *Id.*

basis.[3] An example of the tracking reports which are compiled were exposed in an investigation over a multiyear investigation:



THE MADISON SQUARE GARDEN COMPANY

[redacted]

Summary:

This report is to confirm how [redacted] went from her original seat in Section 102, Row 8, and Seat 5 to Section 1 and Row 1. On January 10, 2022, [redacted] had tickets forwarded to her by MSG employee [redacted] – [redacted] in Section 102, Row 8, and Seat 5-6 for the New York Knicks vs San Antonio Spurs game. A review of CCTV showed [redacted] bring down [redacted] and her female guest down to the Delta club and later escorted them to Section 1 and Row 1 **(See Timeline Highlighted in RED)**.

Searches of [redacted] social media accounts revealed she attended the New York Knicks vs San Antonio Spurs game on January 10, 2022, and CCTV confirmed she was in attendance **(Appendix U)**.

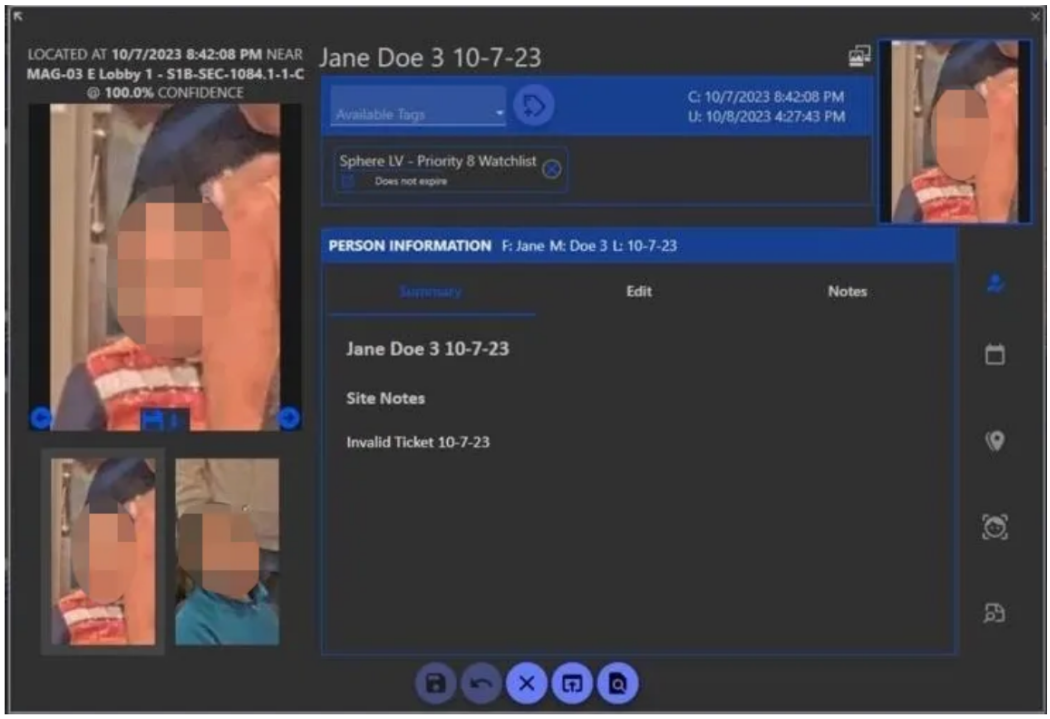
Time:	CAM:	Timeline:
		January 10, 2022
07:09:40	0174	[redacted] enters from the South Con
07:10:20	0241	[redacted] scans her ticket to Section 102, Row 8, Seat 5
07:10:44	0241	[redacted] is seen on the top of South Con elevator
07:11:14	1434	[redacted] goes up the terrace escaltors on level 3 to level 6 concourse
07:11:53	0548	[redacted] is on level 6 concourse
7:12:41	0677	[redacted] enters VOM 102-103

TMG Page | 1

[3] *Id.*

21. Defendant even has an "MSG Threat Management Department" which carries out some or all of this work.[4] According to the investigation by WIRED, Defendant deployed an initial $6 million investment into a company called Xtract One which eventually started to run a facial recognition software called eConnect through the metal detectors with cameras built by Xtract One and funded in-part or entirely by Defendant.[5]

22. According to the investigation, Defendant's security apparatus or other systems nominate which faces should be on eConnect's watch list and assigns a threat score to each; stating, "[t]he score determines if someone is likely to be casually observed from afar, get a not-so-friendly welcome from an [MSG] security officer, or get banned outright,"[6] Defendant even collects biometric data and places children on its watchlist, which can be seen below:



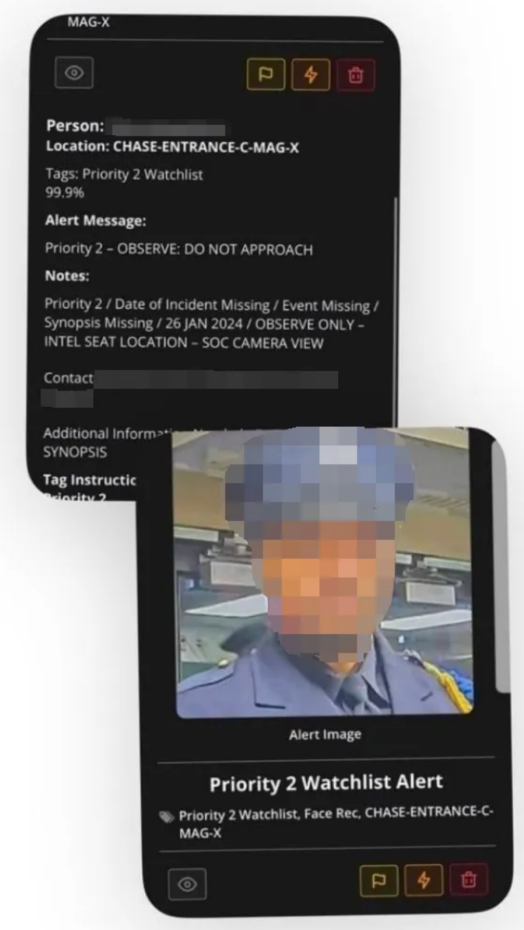
[4] *Id.*

[5] *Id.*

[6] *Id.*

23. The above child, who entered one of Defendant's properties in October of 2023, was given a threat assessment score of "Priority 8 Watchlist" due to a purportedly invalid ticket with "100% confidence."[7]

24. Another profile of an individual from WIRED's investigation was also exposed; it tied the facial recognition data to a former employee, who was currently a member of the New York City Police Academy (and eventually a member of the NYPD) beginning in July of 2024.[8] A portion of profile of that individual, which can be seen below, was assigned a "Priority 2 Watchlist" score with an alert which said in caps "OBSERVE: DO NOT APPROACH":



[7] *Id.*

[8] *Id.*

25. XtractOne, according to WIRED, creates profiles automatically flagging people whose social media posts are unfavorable to Defendant; as the CEO of XtractOne states, "I can pull his picture right off social media. I can feed it into our database, our eConnect database. Now we can get awareness of that person as he approaches the building."[9]

26. Defendant's former employees, including former security staffer Donnie Ingrasselino, have also admitted that they have "perform[ed] fill and intrusive background checks, surveillance, and assessments into individuals' private backgrounds who were of no threat to MSG."[10]

27. This is the sort of data which was compromised in the Data Breach – an amalgamation of biometric driven and sensitive information compiled to create threat assessments for Defendant.

28. As a condition of providing the PII, Plaintiff and Class members to Defendant, Plaintiff and Class members entrusted that Defendant would only use their data for business purposes in a way that was safe and secure. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' PII, Defendant assumed legal and equitable duties and knew that it was responsible for ensuring the security and safety of Plaintiff's and Class members' PII to protect it from unauthorized disclosure and exfiltration.

29. Plaintiff and the Class members relied on Defendant to keep their PII confidential and securely maintained, and only to make *authorized* disclosures of this information, which Defendant failed to do. Defendant collected much more information than it needed to, and this data includes the identifying information of Plaintiff and Class members at a minimum – but, at a

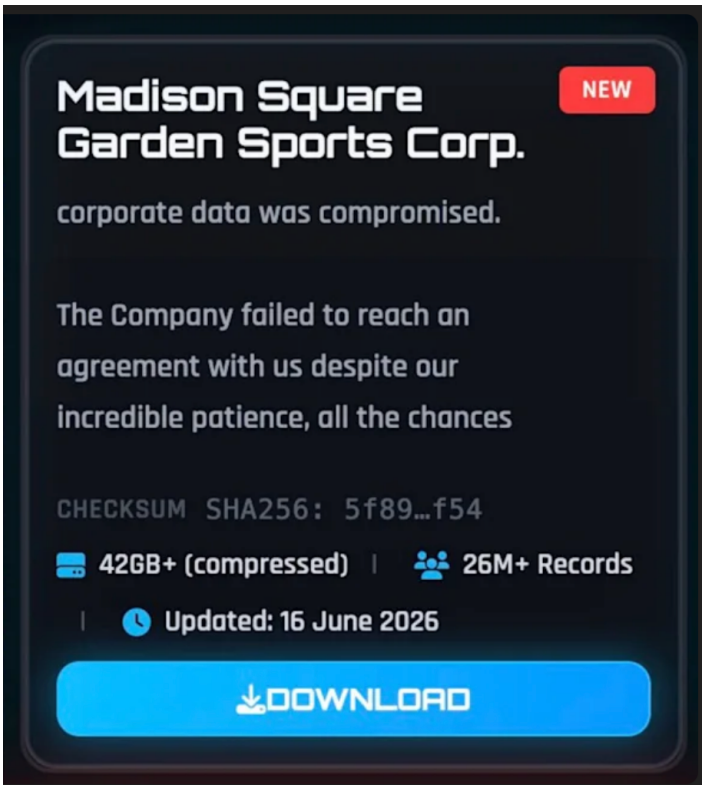
[9] *Id.*

[10] *Id.*

maximum, the biometric facial recognition data, surveillance information, and background check information (which could include credit scores and/or Social Security numbers) which was contained in threat assessment profiles and/or in the corpus of data that included the information of over 26 million visitors to the Arena. This remains dangerously unclear for Plaintiff and Class members due to the lack of transparency by Defendant.

The Data Breach

30. On June 16, 2026, the notorious cybercriminal organization called ShinyHunters announced their infiltration into MSG's computer networks – stating, we have "*It's very simple. When you pay us, your data is deleted, and you move on with your life. When you don't pay us, you get posted here, among other things.*" That same day, the following publication appeared on ShinyHunters' Data Leak Site ("DLS") which contains over 42 GB of compressed data and over 26 million consumer records:



31. To date, there are several categories of PII which are known through a sample observed through media accounts: (1) threat assessment reporting (as two profiles were revealed in the sample – including for celebrity actor Ben Stiller who was marked as a "low risk" in his threat assessment profile), (2) address information, (3) information on celebrities, (4) internal documents about the costs to secure talent, and (5) contact information for talent and their representatives' information. Additionally, there are the profiles of over 26 million individuals which have been compromised, which means that consumers over at least the past few years have had their information leaked as a result of the Data Breach – as it was for the two threat assessment profiles in the sample.

32. Further, there are the internal correspondence about the concerns of consumers emailing Defendant about their facial recognition data being collected, used and retained.

33. While the entirety of the corpus of the PII remains unclear, what is clear is that the data exposed includes over 26 million lines of consumer information – and that the sample of the types of data leaked included risk assessment profiles/dossiers which have been detailed as being tied to biometric facial recognition profiles combined with the consumer's name and other sensitive demographic and characteristic information which allowed Defendant to assign a risk assessment to each individual which enters into the Arena.

34. It is likely that the Data Breach happened because Defendant was not adequately monitoring its systems for breaches; to this point Defendant likely only became aware of the Data Breach because of the ransomware which locked their systems and collected the PII until a ransom was paid.

35. Defendant's response to the Data Breach has been woefully insufficient.

36. *First*, Defendants have yet to disseminate notification letters to victims so that those unaware of the Data Breach can take action to protect themselves (i.e. freezing credit reports, etc.). This will hamstrung millions of people who entrusted Defendant with their PII only to have it compromised – thus, there are an untold number of victims who have any idea that they are in fact victims of the Data Breach. This is compounded by the fact that Defendant has been unclear about or unaware of the Data Breach. *Next*, Defendants have offered zero remediation for the Data Breach whatsoever – so all of the costs of taking preventative action, such as paying for credit monitoring, are costs that are borne by the victims as opposed to the billion-dollar corporate Defendant. *Finally*, Defendant has yet to disclose the full nature of the breach and whether the information that Defendant still has in its control is now in fact secure. This leaves victims with zero reassurance that Defendant has taken steps to protect their PII from being exposed yet again due to Defendant insufficient cybersecurity apparatus.

37. On information and belief, the PII compromised in the files accessed by hackers was not encrypted. This can also be inferred given that the hacker was able to access the data that was listed as compromised in the reporting on the Data Breach.

38. Moreover, the removal of PII from Defendant's systems demonstrates that this cyberattack was targeted by the hacker due to Defendant's status as a large entertainment corporation which was collecting more sensitive information than it probably should have been. Armed with this PII, data thieves, like the hacker in this Action (as well as downstream purchasers of the stolen PII), can commit a variety of crimes, including: phishing attacks, use of sensitive information to steal identities, and, if biometric facial recognition was compromised, using that data for a whole host of harmful activities – as facial template data is as unique as the human fingerprint.

39. To date, victims cannot even trust that the PII compromised in the Data Breach is sufficiently disclosed; this means that all sorts of sensitive information compiled by Defendant and by Defendant's surveillance system for the purpose of creating dossiers on Plaintiff and Class members still remains unknown to the victims.

40. Due to Defendant's flawed security measures and incompetent response to the Data Breach, Plaintiff and the Class members now face a present, substantial, and imminent risk of fraud and identity theft and must deal with that threat forever.

41. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII, and despite Defendant's generous operating budget on security and other investments like their $6 million investment into XtractOne, Defendant provided unreasonably deficient protections prior to the Data Breach, including but not limited to a lack of security measures for storing and handling PII, as well as inadequate employee training regarding how to access, oversee the protection, handle and safeguard for this sensitive set of information.

42. Defendant failed to adequately adopt and train its employees and third-parties on even the most basic of information security protocols, including storing, locking, encrypting and limiting access to current and former consumers and employees' highly sensitive PII; implementing guidelines for accessing, maintaining, and communicating sensitive PII; and protecting sensitive PII by implementing protocols on how to utilize such information.

43. Defendant's failures caused the unpermitted disclosure of Plaintiff's and Class members' PII to an unauthorized third-party cybercriminal organization, namely ShinyHunters, and put Plaintiff and Class members at serious, immediate, and continuous risk of identity theft and fraud.

44. The Data Breach that exposed Plaintiff's and Class members' PII was caused by Defendant's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes.

45. Defendant, despite being a technologically advanced organization, failed to comply with basic security standards or to implement security measures that could have prevented or mitigated the Data Breach.

46. Defendant failed to ensure that all personnel with access to its current/former consumers' PII were properly trained in retrieving, handling, using and distributing sensitive information. Further, there have been no assurances offered by Defendant that all personal data or copies of the PII at issue were either recovered, destroyed, or otherwise protected by an enhanced data security protection apparatus.

The Breach Was Foreseeable

47. Defendant has significant obligations created by industry standards, common law, and its own promises and representations to keep PII confidential and to protect it from unauthorized access and disclosure.

48. Plaintiff and Class members provided their PII to Defendant with the reasonable expectation and mutual understanding that a sophisticated corporation like Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

49. Defendant's data security obligations were particularly acute given the substantial increase in ransomware attacks and/or data breaches in various industries (especially including the entertainment services industry) preceding the date of the Data Breach – including Defendant itself.

50. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

51. Cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

52. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners. PII can be used to distinguish, identify or trace an individual's identity. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as the information compromised in the Data Breach.

53. Given the nature of the Data Breach, it is foreseeable that the compromised PII can (and likely will) be used by hackers and cybercriminals in a variety of different ways.

54. Cybercriminals who possess the Class members' PII can readily obtain Class members' tax returns or open fraudulent credit card or other types of accounts in the Class members' names.

55. The increase in such attacks, and attendant risk of future attacks, was widely known.

56. As such, this specific Data Breach was foreseeable. Defendant was cognizant of data breaches because of how common and high-profile data breaches have become with respect to consumer-facing businesses such as Defendant.

Defendant Failed to Follow FTC Guidelines,
Basic Notions of Privacy and Industry Standards

57. Experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the data which they collect and maintain. The

reason this data is so valuable is because it contains PII, which can be sold and weaponized for purposes of committing various identity theft-related crimes. It is well-known that, because of the value of this data and PII, businesses that collect, store, maintain, and otherwise utilize or profit from PII must take necessary cybersecurity safeguards to ensure that the data they possess is adequately protected.

58. Government agencies also highlight the importance of cybersecurity practices. For example, the Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

59. According to the FTC, the need for data security should be factored into all business decision-making.

60. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

61. The guidelines note that businesses should protect the personal 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.

62. The guidelines also recommend that businesses use an intrusion detection system to detect and 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.

63. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

on the network; and verify that third-party service providers have implemented reasonable security measures.

64. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, in some cases treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential 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 explicate and clarify the measures businesses must take to meet their data security obligations.

65. Defendant failed to properly implement some or all of these (and other) basic data security practices.

66. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

67. Defendant also collected and collects facial recognition information from children, which is a clear violation of the privacy rights of children who attend the Arena.

68. Defendant was at all times fully aware of its obligation to protect PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

69. Experts studying cyber security routinely identify consumer-facing businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

70. Several best practices have been identified that, at a minimum, should be implemented by major entertainment businesses such as Defendant, including but not limited to: educating all employees about cyber security; requiring strong passwords; maintaining multi-layer

security, including firewalls, anti-virus, and anti-malware software; utilizing encryption; making data unreadable without a key; implementing multi-factor authentication; backing up data; and limiting which particular employees can access sensitive data.

71. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; and training staff regarding critical points.

72. These foregoing frameworks are existing and applicable industry standards. Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Breaches of Its Own Obligations

73. Defendant breached its obligations to Plaintiff and Class members and was otherwise negligent and/or reckless because it failed to properly maintain, oversee and safeguard relevant computer systems, network and data – in addition to negligent and/or reckless acts when collecting and retaining data which was not necessary for business operations. In addition to its obligations under state and common law, Defendant owed a duty to Plaintiff and the Class members to exercise reasonable care when obtaining, retaining, securing, safeguarding, deleting, and protecting the PII it collected from being compromised, lost, stolen, accessed or misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including complying with industry standards and requirements, training for its staff and ensuring that their collective computer systems, networks, and protocols adequately protected the PII of Plaintiff and the Class members.

74. Defendant wrongful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect current or former consumers' PII;

c. Failing to properly monitor third-party data security systems for existing intrusions, brute-force attempts and clearing of event logs;

d. Failing to ensure that all third-parties apply all available and necessary security updates;

e. Failing to ensure that all third-parties install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to ensure that all third-parties practice the principle of least-privilege and maintain credential hygiene; and failing to avoid the use of domain-wide, admin-level service accounts;

g. Failing to adequately oversee third-party vendors;

h. Failing to ensure that all third-parties employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

i. Failing to properly train and supervise third-parties in the proper handling of inbound emails.

75. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Defendant negligently and wrongfully failed to safeguard Plaintiff's and Class members' PII.

76. Accordingly, as further detailed herein, Plaintiff and Class members now face a substantial, increased, and immediate risk of fraud, identity theft, and the disclosure of their most sensitive personal information.

Data Breaches are Disruptive and Harm Victims

77. The United States Government Accountability Office ("GAO") 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."

78. That is because all victims of a data breach may be exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it because there is (unfortunately) a market for personally identifiable information, like the PII compromised by the Data Breach.

79. Cybercriminals do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate individual pieces of data an identity thief obtains regarding a person, the easier it is for that thief to take on the victim's identity, or otherwise harass or track the victim.

80. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information regarding a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

81. A stolen Social Security number is a skeleton key to the victim's identity – and, therefore, the type of data that cyberthieves seek. Identity thieves can use a Social Security number for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, fraudulently obtaining a job, fraudulently renting a house, or filing a false police report. The same holds true for biometric information, like facial recognition data.

82. Because of the threat of these harms, the FTC recommends that identity theft 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 (and potentially obtaining an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

83. Theft of PII is gravely serious.

84. PII is an extremely valuable property right.

85. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates that PII has considerable market value.

86. According to the GAO:

> [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.

See GAO Report, at p. 29.

87. Private information, such as the PII compromised herein, is such a valuable commodity to identity thieves that once the information has been compromised, criminals often

trade the information on the "cyber black-market" for years. The private information of consumers remains of high value to criminals, as evidenced by the prices paid through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, private information (inclusive of a Social Security number) can be sold at a price from $40 to $200, and bank details have a price range of $50 to $200. Experian reports that a stolen credit card or debit card number can sell between $5 to $110 on the dark web. Clearly, all this data has real value – which is why it was targeted and stolen in the first place.

88. Because of the value of the PII compromised in the Data Breach, there is a strong probability that entire batches of information stolen in the Data Breach have been dumped on the black market, as that is the *modus operandi* of cybercriminals who perpetrate data breaches, while other batches have yet to be dumped on the black market, meaning Plaintiff and Class members are at a substantial imminent risk of injury including an increased risk of fraud and identity theft for many years into the future.

89. Thus, Plaintiff and Class members must vigilantly monitor their financial, medical, and other accounts and other indices of identity theft (*i.e.*, the mail, email, etc.) for many years to come.

Harm to Plaintiff and the Class

90. Plaintiff attended one or more events at the Arena over the past year and had his biometric information collected (and, therefore, a threat assessment evaluation taken) by Defendant.

91. Plaintiff suffered actual and/or imminent injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) actual or immiment misuse of his compromised PII; (b) actual or imminent damage to and diminution in the value of his PII, a form

of property that Defendant obtained from Plaintiff; (c) an actual or immiment violation of his privacy, including the compromise of highly sensitive PII such as, for example, his sensitive information in combination with his identifying information; (d) imminent and impending injury arising from the increased risk of identity theft and fraud; and (e) losses including the loss of time, as Plaintiff has spent time dealing with the repercussions of the Data Breach, due to time spent mitigating the actual and potential harms caused by the Data Breach.

CLASS ALLEGATIONS

92. Plaintiff Avalos brings this nationwide class on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure. The "Class" that the Plaintiff seeks to represent is defined as follows:

> **Class Definition.** All persons in the United States whose PII was maintained by Defendant and was compromised in the Data Breach.

93. Excluded from the Class are Defendant and Defendant's subsidiaries, affiliates, officers and directors, and any entity in which the Defendant has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

94. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

95. **Numerosity**. Upon information and belief, there are at least millions of additional victims of this Data Breach spread out throughout the United States. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

96. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost or disclosed Plaintiff's and Class members' PII;

b. Whether Defendant (and/or its third-party vendors) 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 Defendant's (and its third-party vendors') data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's (and its third-party vendors') 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 to safeguard their PII;

f. Whether Defendant breached its duty to Plaintiff and Class members to safeguard their PII;

g. Whether computer hackers obtained Plaintiff's and Class members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its (and its third-party vendors') data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's acts, inactions, and practices complained of herein amount to common law negligence;

k. Whether Defendant failed to provide notice of the Data Breach in a timely and proper manner; and

l. Whether Plaintiff and Class members are entitled to damages, civil penalties, punitive damages, equitable relief and/or injunctive relief.

97. **Typicality**. Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by Defendant's uniform conduct. Plaintiff

is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

98. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Class in that they have no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of the other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel experienced in complex class action litigation, including, but not limited to, data privacy class action litigation, and Plaintiff intends to prosecute this action vigorously.

99. **Superiority of Class Action**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based upon an identical set of facts. Without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

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

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

102. **Predominance**. The issues in this action 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. Defendant has engaged in a common course of conduct toward Plaintiff and Class members. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these issues in a single action has important and desirable advantages of judicial economy.

103. This proposed class action does not present any unique management difficulties.

COUNT I

NEGLIGENCE

104. Plaintiff and the Class repeat and re-allege each and every allegation as if fully set forth herein.

105. Defendants owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiff and the Class, managed and stored. This duty arises from multiple sources.

106. Defendants owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target Defendants databases because it contained millions of individuals' valuable PII and, Defendants further knew that, should a breach occur, Plaintiff and the Class would be harmed. Defendants alone controlled its technology, infrastructure, digital platforms, and cybersecurity that were exposed during the Data Breach and allowed hackers to breach and steal information from its database.

107. It further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Defendants knew or

should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen, and that individual need would continue long after the Data Breach ended. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Defendant's unsecured, unreasonable data security measures.

108. Defendant, furthermore, assumed a duty to protect individuals' data by soliciting sensitive PII, collecting that data, and storing that data in its own databases. In fact, Plaintiff and the Class were required to provide PII in order to obtain employment or apply to attend Defendants. Defendant was the only entity capable of implementing reasonable measures to protect Plaintiff's and the Class's sensitive data.

109. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendants to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Defendant's duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by entities like Defendant of failing to implement and use reasonable measures to protect sensitive data. Defendant, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendants' duty to adequately protect sensitive information. By failing to implement and use reasonable data security measures, Defendants acted in violation of § 5 of the FTCA.

110. Defendant is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Defendant to exercise reasonable care with respect to Plaintiff and the Class by implementing

reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, Defendant was the only entity capable of adequately protecting the data that it alone solicited, collected, and stored.

111. Defendant breached its duty to Plaintiff and the Class by implementing unreasonable data security measures that it knew or should have known could cause a Data Breach. Defendant recognized the need to keep PII confidential and safe from cybercriminals who targeted it. Despite that, Defendants implemented unreasonable data security that allowed a single hacker to breach its systems, gain control over them, access its database, and exfiltrate data on millions of individuals, all undetected.

112. Defendant were fully capable of preventing the Data Breach. Defendants were or are sophisticated entities that knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented and used, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. Defendants thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

113. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes. Plaintiff, therefore, seeks all remedies available under the law for Defendants negligence.

COUNT II

NEGLIGENCE PER SE

114. Plaintiff repeats and re-alleges each and every allegation as if fully set forth herein.

115. Defendant's unreasonable data security measures and failure to timely notify Plaintiff and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which Defendant failed to do.

116. Section 5 of the FTCA, 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 entities like Defendant of failing to implement and use reasonable measures to protect individuals' sensitive data. The FTC publications and orders described above also form the basis of Defendants' duty.

117. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PII and sensitive data and by not complying with applicable industry standards. Defendant conduct was particularly unreasonable given the sensitive nature and amount of data it stored on its databases and the foreseeable consequences of a Data Breach should Defendant fail to secure its systems.

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

119. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect. 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 type of harm suffered by Plaintiff and the Class.

120. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury. Plaintiff, therefore, seeks all remedies available under the law for Defendants' negligence per se.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on his own behalf and on behalf of all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action, appointing Plaintiff as the lead plaintiff in this Action, and appointing Plaintiff's below-listed counsel as lead counsel in this Action;

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

C. For an award of equitable and injunctive relief;

D. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the Class which remains in Defendant's possession;

E. For an award of attorneys' fees and costs;

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

G. For such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

121. Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: June 16, 2026

Respectfully submitted,

/s/Blake Hunter Yagman

Blake Hunter Yagman
YAGMAN PLLC
626 RexCorp Plaza
Uniondale, New York 11556
Tel.: (929) 709-1493
Email: *blake.yagman@yagmanpllc.com*

Counsel for Plaintiff Avalos
and the Proposed Class