**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

| | |
|---|---|
| JAMES LANHAM, on behalf of himself and all others similarly situated,<br><br>*Plaintiff*,<br><br>v.<br><br>MLB ADVANCED MEDIA, L.P.,<br><br>*Defendant.* | Case No. _____<br><br>CLASS ACTION COMPLAINT<br><br>DEMAND FOR JURY TRIAL |

Plaintiff James Lanham ("Plaintiff"), on behalf of himself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against the above-captioned Defendant, MLB Advanced Media, L.P. ("Defendant" or "MLB") upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of his counsel as follows:

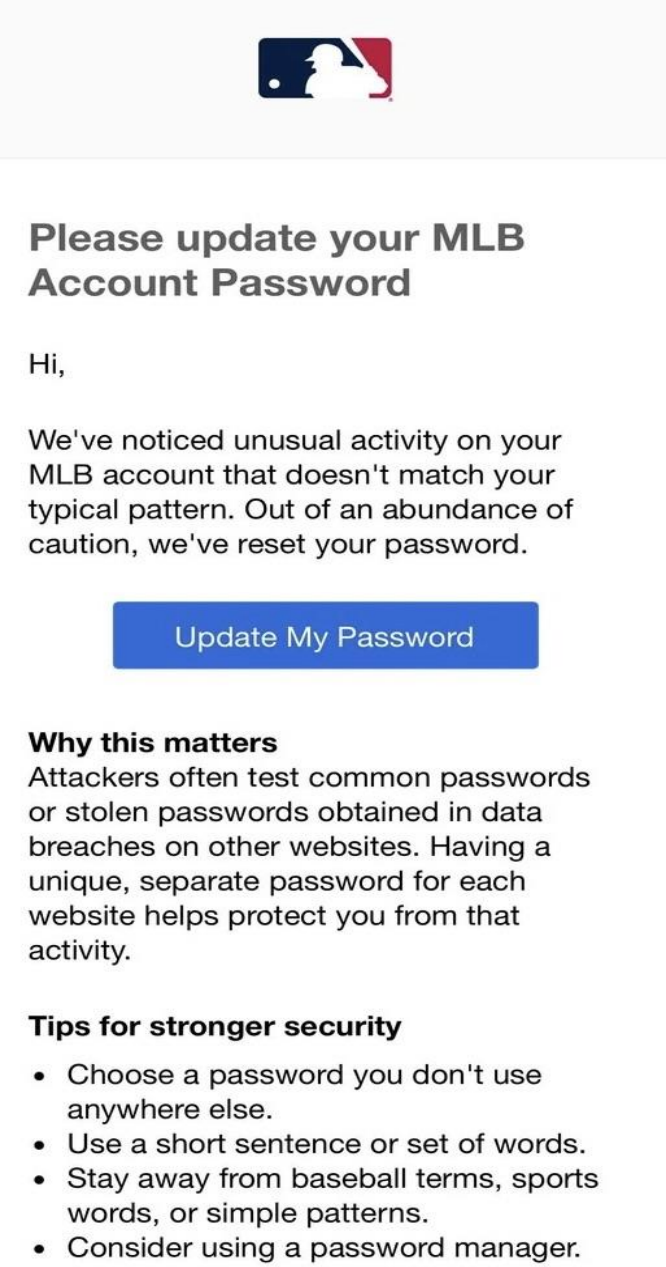
## INTRODUCTION

1. For over a century, Major League Baseball's ballparks have served as America's quintessential gathering place and public square. As the times have changed throughout the history of baseball, so too has the technology that has supported the game itself. One key example of this, and the subject of this Action, is the shift from purchasing baseball tickets at a box office and instead purchasing those same tickets digitally. Today, a majority of baseball tickets are sold through internet-powered mobile applications and websites – with the primary source of those digital transactions funneling into MLB's mobile application, the MLB Ballpark Application (hereinafter, the "MLB Ballpark App").

2. Ultimately, the MLB Ballpark App, which is designed, promoted, and utilized by MLB, acts as a wallet to hold baseball tickets digitally for the purpose of accessing the thirty stadiums owned by MLB's baseball clubs through scanning mechanisms at the entrance of each stadium. Because the sale of baseball tickets comprise the majority of revenue earned by MLB and its thirty baseball clubs, the MLB Ballpark App is a critical infrastructure that facilitates baseball's largest profit generating modality on one hand, and, on the other, the ability for consumers to enjoy and take part in America's pastime.

3. However, digital platforms are not infallible – the MLB Ballpark App, advertised and promoted to fans by MLB as the way to "keep your tickets safe" and the "secure" way to purchase, protect, and use digital baseball tickets, is no exception. Beginning as early as the 2025 MLB Season (from March of 2025 through October or November of 2025), the MLB Ballpark App has had systemic cybersecurity breaches which have resulted in the disappearance and/or theft of baseball tickets from fans who purchased them. To compound matters, MLB has failed to expressly or publicly state the existence of any sort of breach of MLB Ballpark App accounts; this has left consumers in the lurch, unable to protect what personally identifying information ("PII") may have been compromised or exposed as well as the baseball tickets that they may have purchased.

4. Thus far, baseball fans, including Plaintiff Lanham, have received direct email correspondence from MLB and/or the baseball club from whom baseball fans purchased tickets regarding cybersecurity lapses. The first email notifies MLB Ballpark App users that MLB has reset their password due to "unusual activity" and warns them of "[a]ttackers [who] often test common passwords or stolen passwords obtained in data breaches," appearing as follows:



**Please update your MLB Account Password**

Hi,

We've noticed unusual activity on your MLB account that doesn't match your typical pattern. Out of an abundance of caution, we've reset your password.

Update My Password

**Why this matters**
Attackers often test common passwords or stolen passwords obtained in data breaches on other websites. Having a unique, separate password for each website helps protect you from that activity.

**Tips for stronger security**

- Choose a password you don't use anywhere else.
- Use a short sentence or set of words.
- Stay away from baseball terms, sports words, or simple patterns.
- Consider using a password manager.

5. This first email takes no responsibility by MLB and offers little explanation as to what might be occurring, other than to shift blame for inadequate cybersecurity measures back to baseball fans themselves. Currently, the MLB Ballpark App, as compared to industry standards, is woefully insufficient in terms of data security protocols to protect baseball fans from anticipated attacks. This includes the absence of two-factor authentication (which would mitigate penetration of MLB Ballpark App accounts by adding a second layer of protection), the lack of a mandatory

delay time (which would protect baseball fans from uninitiated transfers of baseball tickets by giving baseball fans additional time to approve or deny of ticket transfers as opposed to instantaneous transfers), and the option to print tickets from the MLB Ballpark App (which would remove the ability of cybercriminals and hackers to intercept tickets digitally).

6. The second email from MLB's baseball clubs is just as problematic. This email, which has been sent by numerous baseball teams acknowledges "unauthorized transactions" and asks for baseball fans to "review [] account[s] and ensure all tickets appear as expected[.]". The email then states, "[w]hile reviewing your MLB account, if you notice any resale or ticket forward activity you did not initiate, please email us[.]" The email appears as follows:

---

Good afternoon,

Over the past few days, there have been instances where MLB Ballpark app account holders have noticed unrecognized transactions on their ticket accounts. In light of this activity, while MLB works diligently to resolve the issue, we wanted to reach out to you personally to encourage you to review your account and ensure all tickets appear as expected before you arrive at Citi Field.

While reviewing your MLB account, if you notice any resale or ticket forward activity you did not initiate, please email us at **ticket_services@nymets.com.**

Out of an abundance of caution, we recommend all fans reset their MLB account passwords.

You can do so by visiting **https://www.mlb.com/forgot-password**, entering the email address associated with your MLB account, and clicking "reset my password." Please use a new, original password that you have not used - and won't use - anywhere else. You will not be able to use a password you have previously used on your MLB account. Please ensure you log out of any MLB apps and websites and re-login with your new password on any/all devices.

To ensure easy access to your tickets and the most efficient entry to Citi Field this homestand, please add your tickets to your digital wallet prior to arriving at the ballpark.

Looking forward to seeing you at Citi Field – LGM!

---

7. The key concern with this email is two-fold: (1) it evidences MLB's awareness of breaches of MLB Ballpark App user accounts (while offering a lone solution which is entirely placed in the hands of consumers) and (2) that MLB's MLB Ballpark App has zero ability to detect the presence of unauthorized transfers of baseball tickets (and asks baseball fans themselves to confirm there has not been a theft of their tickets).

8. To make matters worse, MLB's response to the unauthorized access of MLB Ballpark App accounts (the "Data Breach") has been unacceptable: (1) MLB has not publicly disclosed the prevalence of these incidents, which leaves consumers completely unable to take any remedial measures unless they happen to see one of the above-mentioned emails, (2) MLB's failure to publicly address the Data Breach leaves MLB Ballpark App users in the dark about whether any of their PII, like their credit card information, has been exposed through these intrusions, (3) MLB has not added additional security measures, inclusive of those stated above (at ¶ 5), in an attempt to head off these incidents from continuing to occur, and (4) MLB has offered no public compensation program or point of contact for fans who may have already lost money as a result of stolen tickets. Many MLB fans travel long distances and pay additional money to make trips to MLB's ballparks a reality – which means many victims of these issues might have lost funds well beyond just the purchase price of tickets.

9. To date, MLB continues to fail to act. And, each day that MLB continues to do so, more baseball fans are falling victim to MLB's failures to secure their tickets. Further, by dragging its feet, MLB allowed cybercriminals to get a running start on harming to Plaintiff and the Class members, rather than accepting responsibility for MLB Ballpark App's defective cybersecurity apparatus. While MLB could have given Plaintiff and Class members the ability to

start taking action to protect themselves, MLB has made and continues to make a conscious decision not to.

10. As such, Plaintiff, on behalf of himself and all others similarly situated, brings this Action for violations of state consumer protection laws, negligence, breach of implied contract and unjust enrichment, seeking restitution, actual damages, statutory damages, injunctive relief, disgorgement of profits and all other relief that this Court deems just and proper.

## JURISDICTION AND VENUE

11. Plaintiff and Class members seek relief under state and common law violations, including injunctive relief, as well as a measure of damages (including punitive or exemplary damages, as well as statutory and trebled damages), disgorgement of profit into a constructive trust, costs of suit, pre- and post-judgment interest and reasonable attorneys' fees, as this Court deems necessary and proper.

12. *Subject Matter and Supplemental Jurisdiction.* This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). Pursuant to CAFA, the amount in controversy exceeds the sum of $5,000,000 exclusive of interests and costs, there are well over 100 putative Class members, and minimal diversity exists because one or more putative Class members are citizens of a different state than at least one Defendant. Namely, Plaintiff Lanham is domiciled in Illinois whereas Defendant is headquartered in New York.

13. *Personal Jurisdiction.* This Court has personal jurisdiction over the litigants because Defendant is headquartered in New York, Defendant's acts or practices were directed toward this State (and thus, Defendant intentionally availed itself of this jurisdiction by choosing to do business here), Defendant is registered to do business in New York, and Defendant knew or

should have known that their MLB Ballpark App is being used throughout the United States by baseball fans, including here.

14. *Venue.* Venue is proper because the Defendant conducts business in this District, Defendant is headquartered in this District, Defendant's acts or omissions were directed toward this District, Class members were harmed here, and a substantial part of the events, acts and omissions giving rise to Class members' claims occurred here.

## PARTIES

### PLAINTIFF

***Plaintiff James Lanham***

15. Plaintiff Lanham is a natural person and is domiciled in Joliet, Illinois.

16. During the 2025 MLB Season, Plaintiff Lanham purchased tickets to a Chicago Cubs home game taking place at Wrigley Field located in Chicago, Illinois. Plaintiff Lanham's purchase took place two weeks prior to the Chicago Cubs home game at-issue, and the tickets were being held in his MLB Ballpark App. On the day of the game, Plaintiff Lanham's tickets disappeared from his MLB Ballpark App which resulted in him having to forgo the first hour of the game, purchase additional tickets for the same game, and spend hours after the game seeking a refund of the purchase price. Plaintiff Lanham is unaware if his PII and other information was also compromised as a result of the failures of the MLB Ballpark App.

17. As a result of Defendant's failure to adequately protect (and offer safeguards to protect) the baseball fans who use the MLB Ballpark, Plaintiff Lanham suffered economic harm as well as lost time.

## DEFENDANT

***Defendant MLB Advanced Media, L.P.***

18. Defendant MLB Advanced Media, L.P. is a Delaware limited partnership with its principal place of business located in New York, New York.

19. According to MLB.com, MLB Advanced Media, L.P. is "the organization that produces and publishes the Official Website of Major League Baseball, which encompasses […] downloadable mobile applications (*e.g.* MLB, Ballpark, MiLB app)[.]"

## FACTUAL ALLEGATIONS

### *Defendant's Business and Collection of PII*

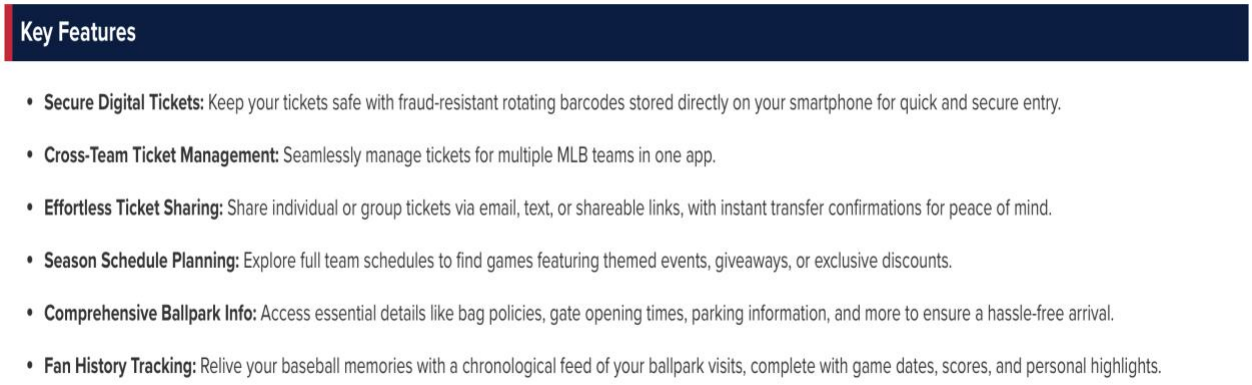
20. Founded in 2000 as a subsidiary of Major League Baseball, MLB Advanced Media, L.P. generates significant amounts of revenue for Major League Baseball each year (approximately $620 million a year in 2012) and, according to Forbes, is "the Biggest Media Company You've Never Heard Of."

21. One of the main lines of business for Defendant is Defendant's ticket-centric MLB Ballpark App.

22. According to MLB.com:

> The MLB Ballpark app streamlines your gameday experience by keeping your digital tickets secure and accessible on your smartphone while helping you plan the perfect gameday. Easily manage, organize, and share your tickets with friends or family for smooth ballpark entry. Browse the full season schedule to find games with special promotions and use detailed ballpark maps to locate your seats, discover the best food spots, and explore all the amenities the ballpark has to offer.
>
> The MLB Ballpark app delivers real-time updates through push notifications about gate openings, weather alerts, concession deals, and other time-sensitive information when users enable push notifications. Designed for both casual attendees and dedicated baseball enthusiasts, it consolidates essential services while adding unique elements to preserve and enhance the live baseball experience.

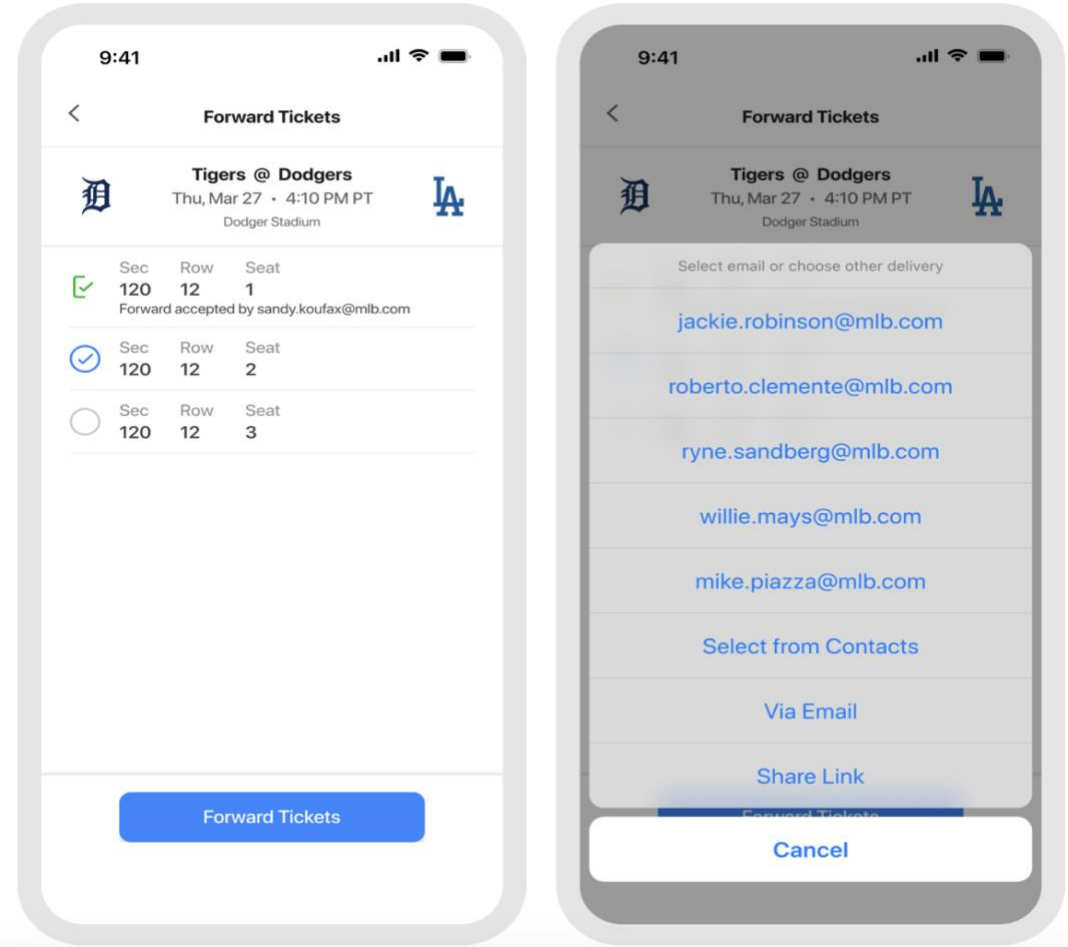
23. Indeed, Defendant highlights six "key features" that the MLB Ballpark App offers baseball fans when they purchase tickets:




24. Notably, one "key feature" is the promise of having "Secure Digital Tickets" because the MLB Ballpark App "[k]eep[s] your tickets safe with fraud-resistant rotating barcodes stored directly on your smartphone for quick and secure entry."

25. Once in the MLB Ballpark App, baseball fans have a number of possible actions that they can take, which include purchasing tickets and transferring tickets to other devices. With respect to purchasing tickets through the MLB Ballpark App, MLB states on its website that "[p]urchasing tickets through the MLB Ballpark app is simple, secure, and guarantees 100% authentic tickets."

26. Additionally, according to the MLB Ballpark App, tickets can be forwarded to other devices instantaneously either through email or via text message, appearing as follows:




27. MLB's MLB Ballpark collects a significant amount of data in the process of allowing consumers to purchase, transfer, and otherwise use digital baseball tickets through the application. According to the MLB.com privacy policy, Defendant may collect:

a. Full name;

b. Email address;

c. Password;

d. Street address;

e. Telephone number(s);

f. Birth date;

g. IP addresses;

h. Location data;

i. Contacts (as stored in a wireless device);

j. Demographic data;

k. Device data;

l. Usage data;

m. Voice recordings;

n. Audiovisual recordings; and

o. Information about interests and preferences.

28. Consistent with the needs of its business as well as Plaintiff's expectations, MLB collects a substantial amount of highly valuable PII. By collecting, using, and deriving a benefit from Plaintiff's and Class members' PII, MLB assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII from unauthorized disclosure.

***The Data Breach***

29. Beginning in August and September of 2025, and during the course of the 2025 MLB Season, reporting and consumer online complaints drew attention to the inadequate and defective cybersecurity protections taken by MLB and its MLB Ballpark App.

30. On September 4, 2025, according to Al Yellon in an article posted on both Yahoo! Sports as well as on "Bleed Cubbie Blue," a Chicago Cubs website which has been in existence for as long as two decades, there were reports of incidents similar to what Plaintiff experienced in Boston, New York, Washington, Baltimore, and Chicago. Additionally, on a Cubs-operated Facebook group tailored to season-ticket holders, there were numerous postings from ticket owners who stated that their MLB Ballpark Apps were hacked and that tickets had been stolen.

31. Yellon continues:

> MLB didn't ask me, but if they did I would also give them this advice: [MLB] should enable two-factor authentication for the MLB Ballpark App (and perhaps also for MLB.com accounts in general. For season-ticket holders like me, there can be thousands of dollars-worth of tickets in the app. Using [two-factor authentication] would put another layer of protection for fans who have purchased those tickets[.]

32. There have been fans all over the country, including in Miami, Los Angeles, Houston, and Philadelphia, report the same issue, including Facebook comments threads with 85 comments of similar experiences as well as a Reddit thread which has 77 comments as well.

33. A major issue, however, has been the inconsistency of outreach by MLB and its baseball clubs to fans – with some fans reporting receiving emails warning them of mandatory password changes as well as "unauthorized access" with others not getting that same warning. Generally, the fans who have received emails received them on September 6, 2025 from the home team of the game for whom they bought tickets, appearing as follows:

> *Dear Fan,*
>
> *Over the past few days there have been a few instances where some account holders have noticed unrecognized transactions on their ticket account. In light of this, we wanted to reach out to encourage you to review your account and ensure all tickets appear in your Ballpark App as expected before you arrive to your upcoming [TEAM] game.*

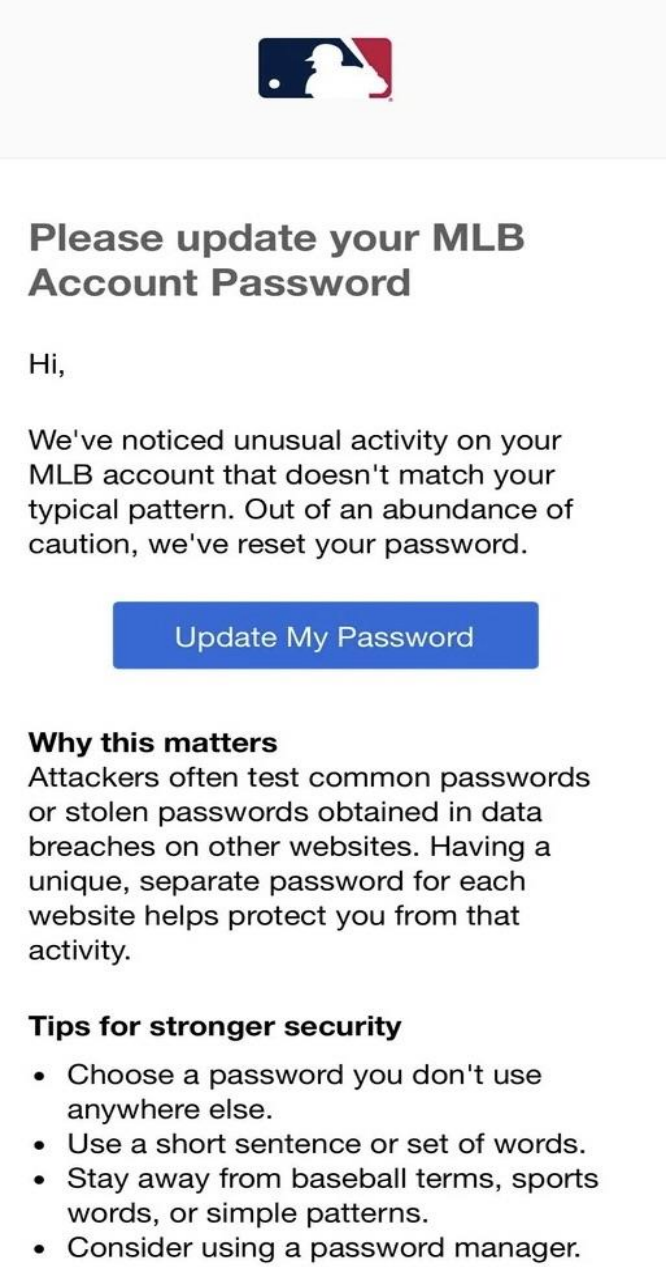
*While reviewing your account, if you notice any resale or ticket forward activity you did not initiate, please email us at [TEAM EMAIL ADDRESS]. Our team is here to help and will respond with a resolution or next steps.*

*Out of an abundance of caution, we recommend all fans reset their MLB account passwords. You can do so by visiting https://www.mlb.com/forgot-password. entering the e-mail address associated with your account, and clicking "reset my password." Please ensure you log out of your account and re-log in with your new password on any/all devices. We encourage you to use a new, original password that you haven't used anywhere else. You will not be able to use a password you have previously used on your account.*

*Thank you for your support and we look forward to seeing you at [STADIUM NAME]*

*[TEAM] © 2025 MLB Advanced Media, L.P. MLB trademarks and copyrights are used with permission of Major League Baseball.*

34. Around the same period of time, MLB has sent emails directly to consumers warning them of unusual activity and the presence of attackers who might be breaching (or have already breached) their accounts:



**Please update your MLB Account Password**

Hi,

We've noticed unusual activity on your MLB account that doesn't match your typical pattern. Out of an abundance of caution, we've reset your password.

Update My Password

**Why this matters**
Attackers often test common passwords or stolen passwords obtained in data breaches on other websites. Having a unique, separate password for each website helps protect you from that activity.

**Tips for stronger security**

- Choose a password you don't use anywhere else.
- Use a short sentence or set of words.
- Stay away from baseball terms, sports words, or simple patterns.
- Consider using a password manager.

35. Taken together MLB's response to the Data Breach has been woefully insufficient.

36. First, MLB has not publicly disclosed the prevalence of these incidents to date, which leaves consumers completely unable to take any remedial measures unless they happen to see one of the above-mentioned emails. This means that many consumers are either unaware of the risks that they might be facing or could even be attributing the loss of tickets to a glitch or a mistake of their own doing.

37. Second, MLB's failure to report the Data Breach to authorities or to publicly address the Data Breach leaves consumers unaware of whether any of their PII (including the information listed at ¶ 27) has been compromised through these intrusions. This makes it nearly impossible for consumers to know what harm they might be facing beyond just the potential theft of baseball tickets.

38. Finally, the attempts to redress and remediate the harm caused by MLB Ballpark App's insufficient data security systems create further harm as well as a risk of future harm. For example, MLB has not added additional security measures, inclusive of those stated above (*e.g.*, applying mandatory two-factor authentication, a period of wait time for transfers and/or the ability to use paper tickets), in an attempt to head off these incidents from continuing to occur. Aside from these very basic measures, MLB has offered no public compensation program or central point of contact for fans who may have already lost money as a result of stolen tickets. And, as previously stated, many MLB fans travel long distances and pay additional money to make trips to MLB's ballparks a reality – which means many victims of these issues might have lost funds well beyond just the purchase price of tickets.

39. MLB failed to disclose specifics of the cyberattack (*i.e.*, how it happened) as well as the specific remedial measures, if any, taken to ensure the protection of tickets and the PII still in MLB's possession. Indeed, MLB told fans to see if their tickets were even still kept within the MLB Ballpark App to ensure they had not been stolen; this means that MLB either does not know the gravity of what has occurred – which means MLB lacks the capacity to taking all of the necessary remedial measures to rectify its deficient cybersecurity apparatus. For victims of the Data Breach, all this information remains unclear.

40. But what is clear from the Notice is that cybercriminals did, in fact, access, view, and exfiltrate Plaintiff's and Class members' tickets and potentially their PII during the period in which the cybercriminals had unfettered access to Plaintiff and Class members' MLB Ballpark App accounts, as that is the *modus operandi* of cybercriminals who commit such attacks.

41. As such, MLB did not implement or maintain adequate measures to protect Plaintiff and Class members' tickets and, potentially, their PII from attackers.

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

43. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks, and despite MLB's generous operating budget, MLB has provided unreasonably deficient protections prior to the Data Breach, including but not limited to a lack of security measures as well as inadequate employee training regarding how to access, handle and safeguard tickets and other potentially compromised information.

44. MLB failed to adequately adopt and train its employees on even the most basic of information security protocols, including: implementation of two-factor authentication, safe storing, account locking, data encryption and limiting access to consumer accounts. These avoidable failures caused the unpermitted disclosure of Plaintiff's and Class members' accounts to an unauthorized third-party cybercriminal(s) and put Plaintiff and Class members at serious, immediate, and continuous risk of identity theft and fraud as well as failing to prevent actual theft of digital property.

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

46. MLB failed to comply with security standards or to implement security measures that could have prevented or mitigated the Data Breach.

***The Breach Was Foreseeable***

47. MLB, especially for an institution of its size and popularity, had weighty obligations created by industry standards, common law, and its own promises and representations made to Plaintiff and Class members to keep their accounts safe as well as their PII confidential from unauthorized access and disclosure.

48. Plaintiff and Class members provided their funds to MLB's ticket partners, baseball clubs, and to MLB itself through the MLB Ballpark App as well as their PII to MLB with the reasonable expectation and mutual understanding that MLB would comply with its obligations to keep such information confidential and secure from unauthorized access.

49. MLB's data security obligations were particularly acute given the substantial increase in data breaches in various industries preceding the date of the Data Breach – including in the ticketing industry. MLB was well aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

50. 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.

51. Items of value and PII is of great value to hackers and cybercriminals, as those items can be resold and the data compromised can be used in a variety of unlawful manners. PII

tied to that data can then 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. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of different ways.

52. Cybercriminals who possess the Class members' PII can potentially make fraudulent purchases or open other types of accounts in the Class members' names.

53. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the sports and ticketing industries, including MLB.

54. Indeed, this specific Data Breach was foreseeable. MLB was cognizant of data breaches because of how common and high-profile data breaches have become with respect to consumer-facing businesses and businesses that provide baseball tickets for millions of fans and employ thousands of people (including cybersecurity professionals), as MLB does.

***Defendant Failed to Follow FTC Guidelines and Industry Standards***

55. 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.

56. 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.

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

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

59. 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.

60. 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.

61. 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.

62. MLB failed to properly implement some or all of these (and other) basic data security practices. MLB's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer accounts and, potentially, to PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

63. MLB was at all times fully aware of its obligation to protect consumer accounts as well as the PII of its consumers. MLB was also aware of the significant repercussions that would result from its failure to do so.

64. 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.

65. Several best practices have been identified that, at a minimum, should be implemented by consumer goods and services providers such MLB, 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.

66. 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.

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

***MLB's Breach of Its Obligations***

68. MLB breached its obligations to Plaintiff and Class members and was otherwise negligent and/or reckless because it failed to properly maintain and safeguard its computer systems, network and data. In addition to its obligations under federal and state law, MLB owed a duty to Plaintiff and the Class members to exercise reasonable care when obtaining, retaining, securing, safeguarding, deleting, and protecting the accounts and/or PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. MLB 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 its computer systems, networks, and protocols adequately protected the PII of Plaintiff and the Class members. This is especially so since MLB repeatedly hails how secure the MLB Ballpark App is.

69. MLB's wrongful conduct may include, 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 consumers' accounts and/or PII;

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

**d.** Failing to apply all available and necessary security updates;

**e.** Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

**f.** Failing to 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 employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

**h.** Failing to properly train and supervise employees in the proper handling of inbound emails.

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

***Harm to Plaintiff***

71. During the 2025 MLB Season, Plaintiff became aware that his MLB tickets were improperly accessed and/or obtained by unauthorized third parties. Later, in September of 2025, MLB and/or one of MLB's baseball clubs indicated that Plaintiff's MLB Ballpark App may have been subject to "unauthorized intrusion" or had been compromised as a result of the Data Breach.

72. As a result of the Data Breach, Plaintiff commenced making reasonable efforts to mitigate the impact of the Data Breach, including but not limited to spending hours trying to seek refunds for his tickets, purchasing new tickets, missing part of the game he had traveled to Wrigley Field for, researching the Data Breach, and, later, reviewing reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

73. Plaintiff (and Class members) suffered actual injury from having the Data Breach including, but not limited to (a) actual loss of value for tickets purchased and then having to repurchase; (b) loss of time; (c) potential violations of their privacy, including the compromise of highly sensitive PII; (d) potential present, imminent and impending injury arising from the increased risk of identity theft and fraud; and (e) additional potential loss of time, beyond the numerous hours that Plaintiff has spent dealing with the repercussions of the Data Breach. These harms would not have occurred but for MLB's failure to monitor and secure its MLB Ballpark App as well as from its unwillingness to remediate these easily fixable security flaws upon discovering them.

## CLASS ALLEGATIONS

74. This Action is properly maintainable as a class action pursuant to Federal Rule of Civil Procedure 23, Rules 23(a), 23(b)(1) and 23(b)(2). Plaintiff brings this class action on behalf of themselves and all other similarly situated individuals. The class which Plaintiff seeks to represent are defined as follows:

> **Class Definition.** All individuals and entities residing in the United States who had tickets during the 2025 MLB Season on their MLB Ballpark App which were subject to unauthorized transfer or theft due to the Data Breach, including all who were sent a notice from MLB about unauthorized or suspicious activity on their MLB Ballpark App accounts due to the Data Breach.

75. 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.

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

77. **Numerosity**. Online reporting evidences that hundreds of consumers fell victim to the Data Breach as described herein. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

78. **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 any Defendant owed a duty to Plaintiff and the Class;

**b.** Whether any Defendant negligently used, maintained, lost, or disclosed Plaintiff's and Class Members' personal information;

**c.** Whether any Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach;

**d.** Whether any Defendant's data security systems prior to, during, and after the data breach complied with the applicable data security standards;

**e.** Whether any Defendant breached a duty to Class Members to safeguard their accounts and/or personal information;

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

**g.** Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of the Defendants' actions or inaction; and

**h.** Whether Plaintiff and Class Members are entitled to damages and/or injunctive relief.

79. **Typicality**. Plaintiff's claims are typical of those of other Class members because Plaintiff's accounts and/or PII, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, were injured by Defendant's uniform conduct. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

80. **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.

81. **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.

82. 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.

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

84. **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 in that all of the victims of the Data Breach had their tickets and/or PII stored on the same computer systems and was unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these issues in a single action has important and desirable advantages of judicial economy.

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

## FIRST CAUSE OF ACTION

## VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349

86. Plaintiff realleges and incorporates by reference all preceding paragraphs 1-85 as if fully set forth herein.

87. New York General Business Law §349 ("New York Gen. Bus. Law § 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

88. Defendant is a business as defined by the statue.

89. Plaintiff and Class members are consumers as defined by the statute.

90. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of New York Gen. Bus. Law § 349. The conduct alleged is a "business practice" as defined by the statute, and the deception occurred in New York state.

91. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Advertising, advancing, promoting, or otherwise stating on its website and in other places that the MLB Ballpark App was "secure" and the safest way to acquire and possess baseball tickets when this information is and was false;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' accounts and/or PII, which was a proximate and direct cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents involving other organizations, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the integrity of Plaintiff's and Class members' accounts including by implementing and maintaining reasonable security measures;

e. Failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' accounts; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security Plaintiff's and Class members' accounts, including duties imposed by the FTC Act, 15 U.S.C. § 45.

92. Defendant's representations and omissions regarding data security were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect their tickets and/or PII.

93. Defendant acted intentionally and knowingly to violate New York's General Business Law, and recklessly disregarded Plaintiff's and Class members' rights.

94. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of tickets; having to purchase new tickets; loss of time; unnecessary expenses related to the Data Breach; a potential increased, imminent risk of fraud and identity theft; potential loss of value of their PII; and the other harms detailed herein.

95. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large. Defendant's violations of the statute have had an impact on the public, including the people of New York, because thousands of New Yorkers had MLB Ballpark App accounts, many of whom have been impacted by the Data Breach.

96. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and Class members that they could not reasonably avoid.

97. As such, Plaintiff and the Class members seek statutory damages in the maximum amount allowed per Class member, or, $50 for each of the victims of the Data Breach.

Additionally, Plaintiff and the Class members seek injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

**SECOND CAUSE OF ACTION**

**NEGLIGENCE/NEGLIGENCE PER SE**

98. Plaintiff realleges and incorporates by reference all preceding paragraphs 1-85 as if fully set forth herein.

99. Defendant required Plaintiff and Class members to download the MLB Ballpark App as well as submit their own non-public personal information in order to purchase goods and services, namely, baseball tickets to the 2025 MLB Season.

100. Plaintiff and Class members are individuals who used the MLB Ballpark App and, therefore, also provided certain PII to Defendant including the PII described above.

101. Defendant had full knowledge of the sensitivity of accessibility to the MLB Ballpark App as well as the PII to which it was entrusted and the types of harm that Plaintiff and Class members could and would suffer if the information were potentially disclosed.

102. Defendant had a duty to Plaintiff and each Class member to exercise reasonable care in holding, safeguarding and protecting their accounts as well as that information.

103. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices.

104. Plaintiff and Class members had no ability to protect their accounts and/or their data in Defendant's possession.

105. By collecting and storing their digital tickets and their data in its computer property, and by sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable

means to secure and safeguard its technology — and Plaintiff's and the Class members' tickets and PII held within it — to prevent theft as well as to safeguard from theft.

106. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a data breach.

107. Defendant owed a duty of care to safeguard the PII of Plaintiff and Class members in its custody. This duty of care arises because Defendant knew of a foreseeable risk to the data security systems it used. Defendant knew of this foreseeable risk because of the explosion of data breach incidents detailed above and in an avalanche of media reports in recent years. Despite its knowledge of this foreseeable risk, Defendant failed to implement reasonable security measures.

108. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements detailed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

109. Defendant was in a 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.

110. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

111. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential accounts, information and/or PII.

112. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Plaintiff's and Class members' accounts and/or PII.

113. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to adopt, implement and maintain adequate security measures and practices to safeguard Plaintiff and Class members' PII;

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

c. Failing to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Plaintiff and Class members' PII;

e. Failing to detect in a timely manner that Plaintiff and Class members' PII had been compromised;

f. Failing to timely notify Plaintiff and Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

114. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff and Class members' accounts and/or PII would result in injury to Plaintiff and Class members.

115. Further, the Data Breach was reasonably foreseeable given the known high frequency of hacking incidents, cyberattacks, and data breaches in the consumer goods and services industry – and, specifically, in the ticketing and sports industries.

116. It was therefore foreseeable that the failure to adequately safeguard Plaintiff and Class members' accounts and/or PII would result in one or more types of injuries to Plaintiff and Class members.

117. Plaintiff and Class members were harmed as a result of Defendant's negligence in the manner alleged herein. Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

118. In addition to monetary relief, Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, as well as to conduct periodic audits of those systems.

## THIRD CAUSE OF ACTION

## BREACH OF CONTRACT

119. Plaintiff realleges and incorporates by reference all preceding paragraphs 1-85 as if fully set forth herein.

120. Defendant provides entertainment services to Plaintiff and Class members. Defendant formed an implied contract with Plaintiff and Class members through their collective conduct.

121. Through the Defendant's provision of goods and services, and its provision of employment opportunities, it knew or should have known that it must protect Plaintiff and Class members' purchases and/or confidential PII in accordance with Defendant's stated policies, industry practices and the applicable law.

122. As consideration, Plaintiff and Class members turned over money and valuable PII in exchange for either entertainment services.

123. Defendant accepted possession of Plaintiff and Class members' money and PII for the purpose of providing goods and services to Plaintiff and the Class members. In delivering their PII to Defendant, Plaintiff and the Class members intended and understood that Defendant would adequately safeguard the PII as part of the provision or receipt of those goods or services.

124. Defendant's implied promises to Plaintiff and Class members include, but are not limited to: (1) taking steps to ensure that anyone who is granted access to PII also protects the confidentiality of that data; (2) taking steps to ensure that the accounts and/or PII placed in control of Defendant's consumers is restricted and limited only to achieve authorized business purposes; (3) restricting access to employees and/or agents who are qualified and trained; (4) designing and implementing appropriate retention policies to protect accounts and/or PII; (5) applying or requiring proper encryption and/or the separation of different data sets; (6) implementing multifactor authentication for access; and (7) taking other steps to protected against foreseeable breaches.

125. Plaintiff and Class members would not have entrusted their accounts and/or PII to Defendant in the absence of such an implied contract.

126. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff and Class members' accounts and/or PII.

127. Plaintiff and Class members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein. Plaintiff seek damages in an amount to be proven at trial.

128. In addition to monetary relief, Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, as well as conduct periodic audits of those systems.

**FOURTH CAUSE OF ACTION**

**UNJUST ENRICHMENT**

**(ON BEHALF OF BOTH CLASSES)**

129. Plaintiff realleges and incorporates by reference all preceding paragraphs 1-85 as if fully set forth herein.

130. This Cause of Action is pled and offered in the alternative to Plaintiff's Third Cause of Action (Breach of Implied Contract).

131. Plaintiff and Class members conferred a benefit upon Defendant with their money and/or PII. Specifically, they purchased goods and services from Defendant. In doing so, they also provided Defendant with their PII. In exchange, Plaintiff and Class members should have received from Defendant the goods and services that were the subject of their respective transactions and also should have had their PII protected with adequate data security.

132. Defendant knew that Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and also used the PII of Plaintiff and Class members for business purposes.

133. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class members' accounts and/or PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own operating profits at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own operating profits over the requisite security.

134. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures.

135. Defendant failed to secure Plaintiff's and Class members' accounts and/or their PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

136. Defendant acquired ticket purchase revenue and/or PII through inequitable means in that it failed to disclose the inadequate security practices detailed herein.

137. Had Plaintiff and Class members known that Defendant had not reasonably secured their accounts and/or PII, they would not have agreed to transact with Defendant.

138. Plaintiff and Class members have no adequate remedy at law.

139. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (a) actual loss of value for tickets purchased and then having to repurchase; (b) loss of time; (c) potential violations of their privacy, including the compromise of highly sensitive PII; (d) potential present, imminent and impending injury arising from the increased risk of identity theft and fraud; and (e) additional potential loss of time, beyond the numerous hours that Plaintiff has spent dealing with the repercussions of the Data Breach. These harms would not have occurred but for MLB's failure to monitor and secure its MLB Ballpark App as well as from its unwillingness to remediate these easily fixable security flaws upon discovering them.

140. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer these and other forms of injury and/or harm.

141. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's goods and services.

## REQUEST FOR RELIEF

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

A. For an Order certifying this case as a class 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

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

**DATED:** Sept. 17, 2025

Respectfully submitted,

/s/ *Blake Hunter Yagman*
Blake Hunter Yagman
**SPIRO HARRISON & NELSON LLC**
40 Exchange Place, Suite 1100
New York, New York 10005
Tel.: 929-709-1493
Email: *byagman@shnlegal.com*

*Attorneys for Plaintiff James Lanham and the Proposed Class*