UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
(EASTERN DIVISION)

JILL LICHTE, on behalf of herself and all others similarly situated, *Plaintiff,* v. **BLUE STAR SECURITY, LLC**, **SECURITY SERVICES HOLDINGS LLC d/b/a PROTOS SECURITY** and **CHICAGO CUBS BASEBALL CLUB LLC**, *Defendants*.	Case No. 1:25-cv-11230 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jill Lichte ("Plaintiff"), on behalf of herself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against the above-captioned Defendants, Blue Star Security, LLC ("Blue Star"), Security Services Holdings LLC d/b/a Protos Security ("Protos") and Chicago Cubs Baseball Club LLC ("Chicago Cubs") (collectively, the "Defendants"), for violations of state law upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of her counsel, as follows.

INTRODUCTION

1. This Action arises from Defendant's unlawful collection, retention, storage and use of Plaintiff and Class members' biometric identifiers [1] and biometric information [2] without obtaining informed written consent or providing consumers with data retention and destruction

[1] "'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10, *et seq*.

[2] "'Biometric information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.*

policies. Specifically, the Chicago Cubs collect biometric identifiers and biometric identifiers from the guests who attend Chicago Cubs games at the historic Wrigley Field located in the Wrigleyville neighborhood of Chicago, Illinois. In order to do this, The Chicago Cubs contract with Blue Star and Protos to collect facial recognition templates from baseball fans at Wrigley Field so that they may be identified through biometric processing systems – namely, Protos' proprietary facial recognition software.

2. Biometric data is particularly sensitive personal information. As the Illinois Legislature has found, "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c) (Illinois' Biometric Information Privacy Act or "BIPA"). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3. In recognition of these concerns over the security of individuals' biometric data, the Illinois Legislature enacted BIPA in 2008, which provides, among other things, that a private entity may not obtain and/or possess an individual's Biometric Data unless it: (1) informs that person (or their representative) in writing that a biometric identifier or biometric information is being collected or stored;[3] (2) informs that person in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used;[4] (3) receives a written release from the person (or their representative) for the collection of

[3] 740 ILCS 14/15(b)(1).
[4] 740 ILCS 14/15(b)(2).

his or her biometric identifier or information;[5] and (4) publishes publicly-available written retention schedules and guidelines for permanently destroying Biometric Data.[6]

4. Further, the entity must store, transmit, and protect from disclosure all Biometric Data using the same standard of care in the industry and in a manner at least as protective as the means used to protect other confidential and sensitive information.[7] No private entity may sell, lease, trade, or otherwise profit from a person's or customer's biometric data.[8] Finally, no private entity may disclose, redisclose, or otherwise disseminate a person's Biometric Data except with the subject's consent, to complete a financial transaction requested by the customer, or other narrowly prescribed situations.[9]

5. In direct violation of the first two provisions of §15 of BIPA (failure to inform regarding collection and failure to inform in writing), as alleged herein, Defendant is and has been actively collecting the biometric data of millions of Chicago Cubs fans who attend baseball games at Wrigley Field.

5. Wrigley Field is outfitted with cameras and advanced video surveillance systems that – unbeknownst to visitors – surreptitiously collects, possesses, or otherwise obtains biometric data. Defendants do not notify visitors of this fact prior to stadium entry, nor do they obtain consent prior to collecting its visitors' Biometric Data.

6. BIPA confers on Plaintiff and Class members a right to know about the inherent risks of biometric data storage, collection, and use, and a right to know how long such risks will persist.

---

5 740 ILCS 14/15(b)(3).
6 740 ILCS 14/15(a).
7 740 ILCS 14/15(e).
8 740 ILCS 14/15(c).
9 740 ILCS 14/15(d).

7. Defendants failed to comply with their critical privacy duties under Illinois law. Defendants do not and does not adequately disclose its biometric data collection practices to its visitors, never obtained written consent from any of its visitors regarding biometric data practices, and never provided any data retention or destruction policies to any of its visitors. Moreover, Defendants invaded Plaintiff's and Class members' privacy through the unauthorized collection, retention, and use of their biometric data.

12. Plaintiff, on behalf of herself and all other Wrigley Field visitors for Chicago Cubs baseball games during the statutory period, brings this Action to prevent Defendants from further violating the privacy rights of visitors to Wrigley Field. Furthermore, Plaintiff brings this action to recover damages for Defendants' unauthorized collection, storage, and use of these individuals' biometric data, as well as reasonable costs and attorneys' fees, pre- and post-judgment interest, as well as injunctive relief.

JURISDICTION AND VENUE

13. This Action is a class action seeking actual damages, restitution, statutory damages, disgorgement of profit, reasonable costs and attorneys' fees, pre- and post-judgment interest, and injunctive relief pursuant to state law – specifically violations of Illinois' Biometric Information Privacy Act (740 ILCS 14/1, *et seq.*), the Illinois Consumer Fraud Act ("ICFA") and the common law doctrine of unjust enrichment.

14. *Subject Matter Jurisdiction.* This Court has subject matter jurisdiction over this Action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this Action (1) involves millions of putative class members; (2) there is minimal diversity between at least one member of the putative Class and Defendants (namely, Plaintiff Jill Lichte is a resident of Illinois

and Protos is headquartered in Connecticut), and (3) in the aggregate, the claims of Plaintiff and the putative Class exceed the sum or value of $5,000,000, exclusive of costs and interest.

15. *Personal Jurisdiction.* This Court has personal jurisdiction over Defendants because both Blue Star and the Chicago Cubs maintain their principal place of business in Illinois. This Court also has personal jurisdiction over Defendants because the events giving rise to this Action occurred in Illinois. Thus, Defendants have continuous and systematic contacts with the State of Illinois, availing itself to the laws of Illinois. Finally, the State of Illinois has an overriding privacy interest to protect the rights of people in Illinois under the State's privacy laws.

16. *Venue.* Venue is proper in this Court under 28 U.S.C. § 1391, because both Blue Star and the Chicago Cubs maintain their principal place of business in this District. Additionally, the conduct giving rise to the allegations and claims asserted in this Action originated and occurred in this District.

PARTIES

Plaintiff Jill Lichte

17. Plaintiff Jill Lichte is domiciled in Illinois.

18. On May 25, 2025, and August 17, 2025, during the statutory period, Plaintiff Jill Lichte attended Chicago Cubs games at Wrigley Field in the Wrigleyville neighborhood of Chicago, Illinois. Plaintiff Lichte did not purchase her own ticket for the baseball games but attended as a guest of another ticket holder. At the games, security services were provided by Blue Star and Protos. When Plaintiff Lichte attended Wrigley Field for the baseball games, Plaintiff Lichte had her facial recognition information unlawfully collected under state law.

Defendant Blue Star Security, LLC

19. Defendant Blue Star Security, LLC is a limited liability company corporation with its corporate headquarters located in Rosemont, Illinois. Defendant Blue Star is a security contractor which employs over 850 active and retired police officers and has provided security services for baseball games hosted by the Chicago Cubs at Wrigley Field since as late as 2023.

20. Defendant Blue Star is a subsidiary or affiliate of Defendant Protos, is a portfolio company which is owned and operated by Southfield Capital. Southfield Capital is a private equity firm located in Connecticut. Southfield Capital, through Defendant Protos, acquired Defendant Blue Star finalized on September 19, 2022.

21. Currently, Defendant Blue Star operates as Defendant Protos' "Specialized Off Duty Division" and has significantly expanded its scope and range of services since being acquired by Defendant Protos.

Defendant Security Services Holdings LLC d/b/a Protos Security

22. Defendant Security Services Holdings LLC d/b/a Protos Security is a limited liability company with its corporate headquarters located in Greenwich, Connecticut. Defendant Protos is owned and operated as a portfolio company of Southfield Capital.

Defendant Chicago Cubs Baseball Club LLC

23. Defendant Chicago Cubs Baseball Club LLC is a limited liability company with its corporate headquarters located at 1060 West Addison Street, Chicago, Illinois 60613. Defendant Chicago Cubs owns Wrigley Field and has employed Defendants Blue Star and Protos since as late as 2023.

FACTUAL ALLEGATIONS

Biometric Data is Uniquely Sensitive and Valuable

24. Biometric technologies, at the most basic level, collect biometric data and use that data to identify or recognize a person based upon some biometric identifier. Specifically, as relevant here, facial recognition technology is a category of biometric technology that analyzes facial features to identify a person.

25. Facial recognition technology operates by detecting an individual's face in person or from an image. A facial recognition technology system then generates a unique faceprint (similar to a fingerprint) by performing an analysis of facial geometry and other features of the face, such as the distance between the nose and the mouth, the shape of the cheekbones, depth of eye sockets, and contour of the lips, ears and chin, among other unique measurements and features.

26. Faceprints generated by facial recognition technology systems may be used by the system to verify a person's identity by conducting a one-to-one comparison. For example, U.S Customs and Border Protection uses facial recognition technology to biometrically confirm the identity of travelers that come to the United States by comparing a photo taken of the traveler at arrival against the passport photo presented by the traveler. Facial recognition technology systems may also compare an individual's face print against a larger database of face prints in order to determine whether the individual matches any person included in the database.

27. As discussed in greater detail below, this is the type of facial recognition system employed by Defendants and that is at issue in this Action.

Defendants' Business

28. The Chicago Cubs are one of the most historic and iconic sports teams in American history. Founded in 1870, Chicago's original baseball team played their first games in Chicago in

1876, before formally becoming known as the Chicago Cubs in 1903. As the Chicago Cubs grew in popularity, Charles Weeghman opened a new stadium in 1914 in the Wrigleyville neighborhood of Chicago which was then-known as Weeghman Park.

29. On April 20, 1916, the Chicago Cubs played their first home game at Weeghman Park. Soon thereafter, in 1921, the stadium was subsequently renamed after chewing gum magnate William Wrigley Jr's acquisition of the team in 1921. From about 1920 through 1926, Weeghman Park was called "Cubs Park" before being renamed to its current name, Wrigley Field, in 1927.

30. Today, Wrigley Field is the second oldest operating Major League Baseball stadium, is a United States Historic Landmark, and seats as many as 41,649 guests at Chicago Cubs home games. The popularity of the Chicago Cubs and Wrigley Field cannot be understated – approximately 37% of visitors to every Chicago Cubs game at Wrigley Field consist of out-of-state guests. Currently, Wrigley Field is one of the most popular sporting venues in the United States.

31. To provide systems of protection, the Chicago Cubs hire Blue Star and Protos to serve as additional security at Wrigley Field during Chicago Cubs games. Largely, Blue Star's deployment of security forces at Wrigley Field consists of former and off-duty Chicago Police Department officers and employees. The Chicago Cubs, at a minimum, play at least 81 baseball games annually at Wrigley Field; this number increases when the team plays additional exhibition games or makes the Major League Baseball playoffs.

The Unlawful Collection and Retention of Biometrics

32. The Chicago Cubs unlawfully surveil guests to Wrigley Field; and, for both visitor and employee protection, use a complex apparatus consisting of software, employee training, and hardware, Wrigley Field deploys mass surveillance inclusive of facial recognition

33. ***Blue Star and Protos Use Facial Recognition at Wrigley Field***. To avoid hiring additional security officers and to minimize shrinkage in Wrigley Field's stores, the Chicago Cubs employ Blue Star and Protos' advanced digital security procedures in order to protect their financial and security interests. To do this, Defendants have owned, operated and used biometric facial recognition software at Wrigley Field during Chicago Cubs games.

34. Indeed, according to Blue Star, it "employs a multi-faceted approach to crowd control [at Wrigley Field.] Advanced technologies such as [closed circuit television] and facial recognition software are utilized to monitor the movements and attendees and identify potential security threats."

35. Additionally, according to Blue Star, Blue Star uses "a combination of physical barriers, access control measures, and vigilant security personnel to prevent unauthorized access. High-tech access control systems, including biometric scanners […] are used to ensure that only authorized personnel can access sensitive areas of the stadium."

36. ***Wrigley Field's Facial Recognition Hardware and Software***. Prior to the 2023 Major League Baseball season, Wrigley Field hired a leading digital security team called Genetec to modernize their security solutions. Together with Genetec, the Chicago Cubs' new security upgrades were "a multi-year restoration effort" which consisted of installing a new control center outfitted by Genetec, as well as its various digital solutions including the Genetec Security Center hardware, as well as the Omnicast and Streamvault software products. According to Genetec, it maintains a system called the "SAFR from RealNetworks" which is a facial recognition system which is "optimized for live video" and specifically integrates into Genetec Security Center – which the Chicago Cubs use.

37. The Chicago Cubs' vice president of security, Doug Lindsay, touted the improvements that Genetec Security Center offered when it was installed in 2023: "[i]n the past,

our security team would have a bunch of different platforms up concurrently. They'd have to know how to find information quickly. On a busy game day, when [we are] managing many different situations, that's hard work. With [Genetec] Security Center, all that information is coming into one platform, so they can see what's happening and focus exclusively on the tasks at hand. We're definitely seeing a higher level of efficiency across our team."

38. According to Genetec, the Chicago Cubs' security team "works 24/7 from their new Joint Operations Center (JOC) managing over 110 camera views thanks to Genetec Omnicast" and that the team "integrated an existing access system in [Genetec] Security Center and deployed 22 Genetec Streamvault appliances." The final phase of the security upgrade involved the "deployment of video analytics in [Genetec] Security Center with the Kiwivision Intrusion Detector, People Counter and Crowd Estimation features."

39. The Chicago Cubs also use facial recognition to enter into its employee section at Wrigley Field.

40. Beginning in 2021, Wrigley Field has used facial recognition through its digital Alvarado eGate hardware through technology provided by Tascent called the Tascent InSight Face system. In order to do this effectively, Tascent deploys its software system called the Tascent Enterprise Suite.

41. Tascent's Alvarado eGate facial recognition cameras appear as follows:

42. According to Tascent, the Alvarado eGate hardware outfitted with Tascent's Insight Face software "provide[s] an intuitive, friendly and streamlined biometric experience to employees as they arrive, enabling them to walk into the office without struggling with an entry pass." Chicago Cubs' vice president for technology, Steve Inman, stated in 2021: "[o]ur experience working with the Tascent team has been extremely positive. The performance of Tascent's system is impressive, and the technical and business flexibility offered by their identity as a service model is a good fit for us." At the time, Tascent agreed. According to Kevin Strouse, Tascent's vice president for solutions and delivery, "[w]e are thrilled that the Chicago Cubs selected Tascent to provide its employees with quick, convenient, and touchless access to their

office. We look forward to assisting the Cubs as they assess how biometrics can contribute further value in support of their business."

43. ***Facial Recognition Employee Training***. To do this, Wrigley Field is outfitted with software which allows Blue Star and other Chicago Cubs employees the ability to deploy facial recognition. For example, the Chicago Cubs currently employ an assistant director of event security named Justin Pagan who has been responsible for software, hardware, and outside vendor support for Wrigley Field's security systems. One such system is called ExacqVision by Exacq, which is a technology platform that integrates facial recognition and face matching systems into existing camera infrastructures. ExacqVision is designed, sold and marketed to consumer-facing businesses by an Irish company called Johnson Controls International PLC. Exacq's website lists Wrigley Field as one of its customers.

44. According to Exacq, their AI analytics "help maintain security, provide operational efficiency, and ensure employee safety […] to customize capabilities such as object classification, behavior and facial recognition for the end-user's specific needs."

45. ***Major League Baseball Privacy Policy***. Major League Baseball's Privacy Policy includes information on its use of biometric information collection from MLB venues – including at Wrigley Field.

46. The Policy states: "[i]f you are a resident of Illinois and elect to participate in any program or offering requiring you to provide biometric information […] MLB will permanently destroy such biometric information, and any information directly derived from such biometric information, when the initial purpose of obtaining such information has been satisfied or within three (3) years following your last interaction with us, whichever occurs first." But this policy is not provided to Wrigley Field attendees, and it does not require their written consent before Major League Baseball collects their biometric information.

47. Additionally, pursuant to the same Privacy Policy, Major League Baseball "limits its use and disclosure of sensitive personal information […] to resist deceptive, fraudulent, or illegal actions [and] to ensure the physical safety of our personnel, customers, visitors and others." According to the Privacy Policy, Major League Baseball collects biometric information and shares it with a "biometric authentication services vendor."

48. While Wrigley Field has its own Privacy Policy, it does not disclose the collection of biometric information at all. Indeed, Wrigley Field never discloses its biometric information collection practices to attendees at any point during visits to its venue, and it does not collect their written consent.

49. As explained below, this misconduct violates federal guidance and state law.

Defendants Violations of Federal Trade Commission Guidance

50. Additionally, Wrigley Field's secretive collection, retention, and use of biometric information demonstrates that the Defendants violate Section 5 of the Federal Trade Commission Act – which protects against deceptive and unfair trade practices.

51. According to the Federal Trade Commission, the collection, retention, and use of biometric information does not, on its face, violate Section 5 of the Federal Trade Commission Act. However, it is considered a deceptive and unfair trade practice when the party collecting the information (here, the Defendants) "[e]ngag[es] in surreptitious and unexpected collection or use of biometric information."

52. In this instance, Defendants fail to adequately disclose the collection of facial recognition data, which violates Section 5 of the Federal Trade Commission Act. Illinois' Illinois Consumer Fraud Act ("ICFA") follows Federal Trade Commission guidance regarding deceptive and unfair trade practices: this means that Defendants' conduct violates ICFA because of the

failure to follow the Federal Trade Commission's guidance with respect to the disclosure biometric information collection.

Illinois's Biometric Information Privacy Act

53. In 2008, the Illinois Legislature enacted BIPA due to the "very serious need [for] protections for the citizens of Illinois when it comes to biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA makes it unlawful for a company to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers biometric information, unless it first:

> (l) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

54. To facilitate these informed notice and consent provisions, Section 15(a) of BIPA also provides:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

55. To enforce BIPA's requirements, the statute includes a private right of action authorizing "[a]ny person aggrieved by a violation" to sue and recover for each violation damages

of $1,000 for a negligent violation, or $5,000 in the event of an intentional or reckless violation, plus attorneys' fees, costs, and appropriate injunctive relief. 740 ILCS 14/20.

56. As alleged below, Defendants' practice of collecting, storing, and using individuals' biometric data without obtaining informed written consent violates all three prongs of §15(b) of BIPA. Defendants' failure to provide a publicly available written policy regarding a schedule and guidelines for the retention and permanent destruction of individuals' Biometric Data also violates §15(a) of BIPA.

57. Wrigley Field's continued use of facial recognition-enabled video surveillance systems demonstrates that the Chicago Cubs have violated and continues to violate BIPA. The Wrigley Field's surveillance system recognizes facial characteristics and features, and captures, collects, and stores biometric data for later use.

58. Unbeknownst to the average baseball fan, and in direct violation of §15(b)(1) of BIPA, the Chicago Cubs scan, collect, and store its biometric information and identifiers in an electronic database. This occurs when customers, or prospective customers, enter into and move throughout the corridors of Wrigley Field. The Chicago Cubs engage in this practice without informing its guests in writing that it is using surveillance technology that collects and stores biometric information.

59. In direct violation of §§15(b)(2) and 15(b)(3) of BIPA, the Chicago Cubs did not inform Plaintiff and Class members – who were subjected to video surveillance recording within Wrigley Field – of the specific purpose and length of term for which their biometrics would be collected, stored, and used, nor did they obtain a written release from any of these individuals.

60. In direct violation of §15(a) of BIPA, the Chicago Cubs do not have an adequate written, publicly available policy identifying their retention schedules or guidelines for permanently destroying any of these biometric identifiers or biometric information.

Plaintiff Lichte's Experience

61. Plaintiff Lichte is an Illinois resident. She has entered Wrigley Field on numerous occasions as a guest of a Cubs ticket holder during the statutory period, including for games on May 25, 2025, and August 17, 2025.

62. On information and belief, each Chicago Cubs game entered into by Plaintiff Lichte utilizes a complex facial recognition-enabled video surveillance system.

63. Plaintiff Lichte did not know that Defendants would collect, obtain, store, and/or use her biometric identifiers or biometric information. Plaintiff Lichte did not give informed written consent to Defendants to collect, obtain, store, and/or use her biometric data, nor was Plaintiff Lichte presented with or made aware of any publicly available retention schedule regarding her biometric data.

64. Likewise, Plaintiff Lichte was never provided with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage, or use of her unique biometric identifiers and/or biometric information.

65. By collecting, obtaining, storing, and using Plaintiff Lichte's biometric data without her consent, written or otherwise, Defendants invaded Plaintiff's statutorily protected right to privacy in her biometric data.

66. In direct violation of §§15(b)(2) and 15(b)(3) of BIPA, Defendants never informed Plaintiff Lichte of the specific purpose and length of time for which her biometric data would be collected, stored, and used, nor did Defendants obtain a written release.

67. In direct violation of §15(a) of BIPA, Defendant does not have an adequate written, publicly available policies identifying their retention schedules or guidelines for permanently destroying any of Plaintiff Lichte's biometric data.

68. Any applicable statute of limitations has been tolled by Defendants' knowing and active concealment of their unlawful conduct. Throughout the Class Period, Defendants affirmatively and fraudulently concealed their unlawful conduct.

69. Plaintiff Lichte's and Class members did not discover, nor could they have discovered through the exercise of reasonable diligence, the existence of the hidden and ambiguous privacy policies and terms of use.

70. Further, the very nature of Defendants' conduct was secret and self-concealing. Defendants used advanced video management systems capable of facial recognition and capturing biometric data and other technologies without adequately informing impacted individuals that their biometric data was being collected and potentially disseminated.

71. As a result of Defendant's fraudulent concealment, all applicable statutes of limitations affecting the claims of Plaintiff Lichte and Class members have been tolled.

72. Defendants' misconduct violated Plaintiff Lichte's privacy, harming her emotionally and depriving her control over how her biometric data is collected and used for surveillance and other unknown purposes.

CLASS ALLEGATIONS

73. 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 Plaintiff seeks to represent is defined as follows:

> **Class Definition.** All individuals who, while in the State of Illinois and during the statutory period, had their biometric data collected, captured, received, obtained, stored, sold, leased, traded, disclosed, redisclosed, disseminated, and/or otherwise profited from and/or used by Defendants without their consent.

The following are excluded from the Class: (1) any Judge presiding over this action and members of his or her family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant has a controlling interest (including current and former employees, officers, or directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; and (5) the legal representatives, successors, and assigns of any such excluded persons.

74. **Numerosity**: Members of the Class are so numerous that their individual joinder is impracticable. Upon information and belief, members of the Class number in the thousands. The precise size of the Class and Class members' identities are unknown to Plaintiff Lichte at this time but may be determined through discovery. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

75. **Typicality**: Plaintiff Lichte's claims are typical of the claims of the Class members because Plaintiff had her biometric data collected, used, and profited from by Defendants upon use of their stores, and therefore, Plaintiff's claims arise from the same common course of conduct giving rise to the claims of the members of the Class and the relief sought is common to the Class.

76. **Commonality and Predominance**: Common and well-defined questions of fact and law exist as to all members of the Class and predominate over any questions affecting only individual class members. These common legal and factual questions include, but are not limited to, the following:

a) whether Defendants collected or otherwise obtained Plaintiff's and the Class's biometric data;

b) whether Defendants properly informed Plaintiff and the Class that it collected, used, and stored their biometric data;

c) whether Defendants obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiff's and the Class's biometric data;

d) whether Defendants developed and made available to the public a written policy establishing a retention schedule and guidelines for permanently destroying biometric data when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of their last interaction, whichever occurs first;

e) whether Defendants used Plaintiff's and the Class's biometric data to identify them;

f) whether Defendants violations of BIPA were committed intentionally, recklessly, or negligently;

g) whether Defendants collection of biometric data was a deceptive or unfair trade practice;

h) whether Defendants were unjustly enriched;

i) whether Plaintiff and members of the Class sustained damages as a result of Defendants' activities and practices referenced above, and, if so, in what amount; and

j) whether Defendants profited from the activities and practices referenced above, and, if so, in what amount.

77. **Adequate Representation**: Plaintiff has retained competent counsel experienced in prosecuting complex consumer class actions. Plaintiff and her counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff and her counsel can fairly and

adequately represent and protect the interests of the Class because their interests do not conflict with the interests of the Class Plaintiff seeks to represent. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Class or additional claims as may be appropriate.

78. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Moreover, even if every member of the Class could afford to pursue individual litigation, the Court system could not. Individual litigation of numerous cases would be unduly burdensome to the courts. Individualized litigation would also present the potential for inconsistent or contradictory judgments, and it would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system, and protects the rights of each member of the Class. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with state law.

COUNT I
Violation of 740 ILCS 15(a)
(Against All Defendants)
On Behalf of Plaintiff and the Class

79. Plaintiff repeats and re-alleges each and every allegation as if fully set forth in paragraphs 1-76.

80. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

81. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendants.

82. Section 15(a) of BIPA requires that:

> [Any] private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.
>
> 740 ILCS 14/15(a).

83. Defendants are corporations and thus qualify as "private entities" under BIPA. *See* 740 ILCS 14/10.

84. Plaintiff and the Class members are individuals who had their biometrics collected and stored by Defendants. *See* 740 ILCS 14/10.

85. Defendants do not provide a written, publicly available retention schedule and guidelines for permanently destroying the biometric data of Plaintiff or Class members, as required by BIPA. *See* 740 ILCS 14/15(a). Defendants' failure to provide such a schedule and guidelines constitutes an independent violation of the statute.

86. Each instance in which Defendants collected, stored, used, or otherwise obtained Plaintiff's and/or members of the Class's biometric data as described herein constitutes a separate

violation of the statutory right of Plaintiff and each Class member to keep private this biometric data, as set forth in BIPA, 740 ILCS 14/1, *et seq.*

87. On behalf of herself and members of the proposed Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendants to comply with BIPA's requirements, including BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein, and for the provision of the requisite written disclosure to consumers; (2) statutory damages of $5,000 for each and every intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or, alternatively, statutory damages of $1,000 for each and every violation pursuant to 740 ILCS 14/20(1) if the violations are found to have been committed negligently; and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT II
Violation of 740 ILCS 15(b)
(Against All Defendants)
(On Behalf of Plaintiff and the Class)

88. Plaintiff repeats and re-alleges each and every allegation as if fully set forth in paragraphs 1-76.

89. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

90. Plaintiff brings this claim individually and on behalf of the members of the proposed Class against Defendants.

91. Section 15(b) of BIPA makes it unlawful for any private entity to, among other things:

> [C]ollect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and

> used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information.

740 ILCS 14/15(b).

92. Defendants are corporations and thus qualifies as "private entities" under BIPA. *See* 740 ILCS 14/10.

93. Plaintiff and the Class members are individuals who had their biometrics collected and stored by Defendants. *See* 740 ILCS 14/10.

94. Defendants systematically collected, used, and stored Plaintiff's and Class members' biometric data derived from Plaintiff's and Class members' facial geometry without first obtaining the written release required by 740 ILCS 14/15(b)(3), and thereby uniformly invaded Plaintiff's and Class members' statutorily protected right to privacy in their biometrics. Likewise, Defendants failed to properly inform Plaintiff or members of the Class in writing that their biometric data was being collected, stored, or otherwise obtained, and of the specific purpose and length of term for which those biometrics were being collected, stored, and used, as required by 740 ILCS 14/15(b)(1)-(2).

95. Plaintiff and the Class have been directly harmed by Defendants' violations of Sections 14/15(a)-(b) of BIPA. They have been deprived of their control over their valuable information and otherwise suffered monetary and non-monetary losses. By depriving Plaintiff and the Class of control over their valuable information, Defendants misappropriated the value of their biometric identifiers and/or biometric information. Based on information and belief, Defendant has profited from its unlawful conduct in several forms, including reducing costs for hiring security, reducing shrinkage (loss of inventory by theft) and saving money on other less intrusive protective measures.

96. Each instance in which Defendants collected, stored, used, or otherwise obtained Plaintiff's and Class members' biometric data as described herein constitutes a separate violation of the statutory right of Plaintiff and Class members to keep private this biometric data, as set forth in BIPA, 740 ILCS 14/1, *et seq.*

97. On behalf of herself and members of the proposed Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendants to comply with BIPA's requirements, including BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein, and for the provision of the requisite written disclosure to consumers; (2) statutory damages of $5,000 for each and every intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or, alternatively, statutory damages of $1,000 for each and every violation pursuant to 740 ILCS 14/20(1) if the violations are found to have been committed negligently; and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT III
Violations of the Illinois Consumer Fraud Act, 815 ILCS 505 (*et seq.*)
(Against the Chicago Cubs)
On Behalf of Plaintiff and the Class

98. Plaintiff repeats and re-alleges each and every allegation as if fully set forth in paragraphs 1-76.

99. Defendants are considered "businesses" under the Illinois Consumer Fraud Act.

100. Defendants' business acts and practices are unfair and deceptive under ICFA because Illinois has a strong public policy of protecting consumers' privacy interests, including their biometric privacy. Defendants violated ICFA by collecting Plaintiff and Class members' biometric data without written consent and did so in order to profit, as explained herein.

101. Defendants' acts and practices are "unfair" in that they are immoral, unethical, unfair, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of Defendants secretly collecting and sharing Plaintiff's biometric data is significant and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiff and many Class members were completely unaware of the full breadth of Defendants' conduct, including the use of their biometric identifier information for profit, they could not have avoided the harm caused by this conduct.

102. Under ICFA, Plaintiff seeks all available remedies, including actual damages, restitution, treble damages, statutory damages, reasonable costs and attorneys' fees, and any other relief this Court deems just and proper.

COUNT IV
Unjust Enrichment/Restitution
(Against Blue Star and Protos)
On Behalf of Plaintiff and the Class

103. Plaintiff repeats and re-alleges each and every allegation as if fully set forth in paragraphs 1-76.

104. Defendant was unjustly enriched by its unlawful misappropriation of Plaintiff's and the Class's Biometric Information. Through its unlawful conduct, Defendant received and retained a benefit it otherwise would not have achieved. By depriving Plaintiff and the Class of control over their valuable Biometric Information, Defendant took control of and misappropriated the value of their Biometric Information. Defendant's conduct also exposed Plaintiff and the Class to a heightened risk of an invasion of their privacy.

105. There is not another adequate remedy at law. It would be unjust and unfair for QuikTrip to retain any of the benefits obtained from its unlawful misappropriation of Plaintiff's

and the Class's Biometric Information. Defendant should be ordered to disgorge the proceeds that it unjustly received from the misappropriation of Plaintiff's and the Class's Biometric Information.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the proposed Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing her counsel as Class Counsel;

B. Declaring that the actions of Defendants, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;

C. Declaring that the actions of Defendant Chicago Cubs, as set out above, violates ICFA, 815 ILCS 505, *et seq.*;

D. Declaring that the actions of Defendants Blue Star and Protos constituted unjust enrichment;

E. Awarding compensatory, non-compensatory, statutory, exemplary, and punitive damages;

F. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, among other things, an order requiring that Defendants ensures its collection, storage, and usage of biometric data complies with BIPA;

G. Awarding Plaintiff and the Class statutory damages of $5,000 for each and every intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), and

statutory damages of $1,000 for each and every negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

H. Awarding Plaintiff and the Class statutory damages of $500 per violation of ICFA pursuant to 815 ILCS 505 for each and every violation of ICFA;

I. Awarding restitution of all monies, expenses, and costs due to Plaintiff and the Class as well as disgorgement of profit into a constructive trust;

J. Awarding Plaintiff and the Class reasonable litigation expenses and attorneys' fees;

K. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and,

L. Awarding such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 17, 2025

Respectfully submitted,

By: */s/ Samuel J. Strauss*

Samuel J. Strauss (SBN: 634033)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com