FILED
8/20/2019 2:00 PM
DOROTHY BROWN
CIRCUIT CLERK
COOK COUNTY, IL
2019CH09603
6252259



**IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS**
**COUNTY DEPARTMENT, CHANCERY DIVISION**

| | | |
|---|---|---|
| **RONNIE ALQUERO, individually, and on behalf of all others similarly situated,** | ) | |
| **Plaintiff,** | ) | **Case No.** 2019CH09603 |
| **v.** | ) | |
| **ELDORADO RESORTS, INC. and ELGIN RIVERBOAT RESORT – RIVERBOAT CASINO d/b/a GRAND VICTORIA RIVERBOAT CASINO,** | ) | **JURY TRIAL DEMANDED** |
| **Defendants.** | ) | Hearing Date: 12/18/2019 9:30 AM - 9:30 AM<br>Courtroom Number: 2402<br>Location: District 1 Court<br>Cook County, IL |

## CLASS ACTION COMPLAINT

Plaintiff Ronnie Alquero ("Alquero" or "Plaintiff"), individually and on behalf of all others similarly situated (the "Class"), by and through his attorneys, brings the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against Eldorado Resorts, Inc. and Elgin Riverboat Resort – Riverboat Casino d/b/a Grand Victoria Riverboat Casino (collectively, "Defendants"), their subsidiaries and affiliates, to redress and curtail Defendants' unlawful collection, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric data. Plaintiff alleges as follows upon personal knowledge as to himself, his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

## NATURE OF THE ACTION

1. Defendants own and operate the Grand Victoria Riverboat Casino, a state-licensed riverboat gambling facility located in Elgin, Illinois. The casino property includes 1,100 slot

machines, 30 table games, a 12-table poker room, four restaurants, and meeting and banquet space, and Grand Victoria Riverboat Casino employs over 700 employees.

2. For purposes of casino security, Defendants grant certain employees access to restricted areas, such as equipment and supply rooms. In order to obtain the keys to these restricted areas, Defendants require employees who are authorized to access those areas, including Plaintiff, to scan their fingerprints on a biometric key dispenser.

3. While many employers use conventional methods for granting access to secure areas (such as keys, ID badges, or key cards), Defendants' employees are required, as a condition of employment, to have their fingerprints scanned by a biometric device and enrolled in an employee database(s).

4. Unlike keys, ID badges, or key cards – which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with each employee. This exposes Defendants' employees to serious and irreversible privacy risks. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Google+, Equifax, Uber, Facebook/Cambridge Analytica, and Marriott data breaches or misuses – employees have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

5. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as Defendants – and financial institutions have incorporated biometric applications into their workplace in the form of biometric security systems, timeclocks or authenticators, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

6. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), *available at* www.opm.gov/cybersecurity/cybersecurity-incidents.

7. An illegal market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and facial photographs – of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259fl38.

8. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than $8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), *available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

9. In the United States, law enforcement, including the Federal Bureau of Investigation and Immigration and Customs Enforcement, have attempted to turn states' Department of Motor Vehicles databases into biometric data goldmines, using facial recognition technology to scan the faces of thousands of citizens, all without their notice or consent. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, The Washington Post (July 7, 2019), *available at* https://www.washingtonpost.com/

technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/?noredirect=on&utm_term=.da9afb2472a9.

10. This practice has been criticized by lawmakers. Some states, including Illinois, have refused to comply with law enforcement's invasive requests. *State Denying Facial Recognition Requests*, Jacksonville Journal-Courier (July 9, 2019), *available at* https://www.myjournalcourier.com/news/article/State-denying-facial-recognition-requests-14081967.php.

11. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS § 14/1, *et seq.*, specifically to regulate companies that collect, store and use Illinois citizens' biometrics, such as fingerprints.

12. Notwithstanding the clear and unequivocal requirements of the law, Defendants disregard Plaintiff's and other similarly-situated employees' statutorily protected privacy rights and unlawfully collect, store, disseminate, and use Plaintiff's and other similarly-situated employees' biometric data in violation of BIPA. Specifically, Defendants have violated and continues to violate BIPA because they did not and continue not to:

a. Properly inform Plaintiff and other similarly-situated employees in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, and used, as required by BIPA;

b. Receive a fully compliant written release from Plaintiff and other similarly-situated employees to collect, store, or otherwise use their fingerprints, as required by BIPA.

c. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated employees' fingerprints, as required by BIPA; and

d. Obtain consent from Plaintiff and other similarly-situated employees to disclose, redisclose, or otherwise disseminate their fingerprints to a third party as required by BIPA.

13. Plaintiff and other similarly-situated employees are aggrieved because they were not: (1) properly informed in writing of the purpose and length of time for which their fingerprints were being collected, stored, disseminated and used; (2) provided a publicly available retention schedule or guidelines for permanent destruction of the biometric data; and (3) provided (nor did they execute) a fully-compliant written release, as required by BIPA.

14. Upon information and belief, Defendants improperly disclosed Plaintiff's and other similarly-situated employees' fingerprint data to at least one out-of-state third-party vendor.

15. Upon information and belief, Defendants improperly disclosed Plaintiff's and other similarly-situated employees' fingerprint data to other, currently unknown, third parties, including, but not limited to third parties that host biometric data in their data center(s).

16. Upon information and belief, Defendants lack publicly available retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated employees' biometric data and have not and will not destroy their biometric data as required by BIPA.

17. Plaintiff and other similarly situated employees are aggrieved by Defendants' failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of Plaintiff's and other similarly-situated individuals' employment with Defendants.

18. Plaintiff and other similarly situated employees have suffered an injury in fact based on Defendants improper disclosures of their biometric data to third parties.

19. Plaintiff and other similarly situated employees have suffered an injury in fact based on Defendants' violations of their legal rights.

20. These violations have raised a material risk that Plaintiff's and other similarly-situated employees' biometric data will be unlawfully accessed by third parties.

21. Defendants' employees have a proprietary right to control their biometric identifiers and/or information. In failing to comply with the requirements of BIPA, Defendants intentionally interfere with each employee's right of possession and control over their valuable, unique, and permanent biometric data.

22. Defendants are directly liable for, and had actual knowledge of, the BIPA violations alleged herein.

23. Accordingly, Plaintiff, on behalf of himself as well as the putative Class, seeks an Order: (1) declaring that Defendants' conduct violates BIPA; (2) requiring Defendants to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

**PARTIES**

24. Plaintiff Ronnie Alquero is a natural person and a resident of the State of Illinois.

25. Eldorado Resorts, Inc. ("Eldorado") is a Nevada corporation with its principal place of business at 100 W. Liberty St., Ste. 1150, Reno, NV. Eldorado owns and operates twenty-eight casino and resort properties, including Grand Victoria Riverboat Casino, throughout the United States in Nevada, New Jersey, Iowa, Colorado, Missouri, Florida, Louisiana, Illinois, Ohio, Indiana, Mississippi, West Virginia, and Pennsylvania.

26. Defendant Elgin Riverboat Resort – Riverboat Casino, d/b/a Grand Victoria Riverboat Casino ("Grand Victoria Riverboat Casino") is a state-licensed gambling facility located at 250 South Grove Avenue, Elgin, Illinois.

27. Eldorado acquired Grand Victoria Riverboat Casino from its previous owners on August 7, 2018.

## JURISDICTION AND VENUE

28. This Court has jurisdiction over Defendants pursuant to 735 ILCS § 5/2-209 because they conduct business transactions in Illinois, have committed statutory violations and tortious acts in Illinois, and are registered to conduct business in Illinois.

29. Venue is proper in Cook County because Defendants are authorized to conduct business in this State and Defendants conduct business transactions in Cook County.

## FACTUAL BACKGROUND

### I. The Biometric Information Privacy Act.

30. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS § 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. *See* 740 ILCS § 14/5.

31. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records – which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used that company's fingerprint scanners were completely unaware that the scanners were not

actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

32. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS § 14/5.

33. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent violations, and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS § 14/20.

34. BIPA is an informed consent statute which achieves its goal by making 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 or biometric information, unless it first:

a. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored or used;

b. 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, or used; and

c. Receives a written release executed by the subject of the biometric identifier or biometric information.

*See* 740 ILCS § 14/15(b).

35. BIPA specifically applies to employees who work in the State of Illinois. BIPA defines a "written release" specifically "in the context of employment [as] a release executed by an employee as a condition of employment." 740 ILCS § 14/10.

36. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and facial geometry, and – most importantly here – fingerprints. *See* 740 ILCS § 14/10. Biometric information is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *Id*.

37. BIPA also establishes standards for how companies must handle Illinois citizens' biometric identifiers and biometric information. *See, e.g.,* 740 ILCS § 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for such disclosures. *See* 740 ILCS § 14/15(d)(1).

38. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information (740 ILCS § 14/15(c)) and requires companies to develop and comply with 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 such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS § 14/15(a).

39. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and – most significantly – the unknown ramifications of biometric technology. Biometrics are biologically unique to the individual and, once compromised, an individual is at a heightened risk for identity theft and left without any recourse.

40. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics. BIPA also protects individuals' rights to know the precise

nature for which their biometrics are used and how they are being stored and ultimately destroyed, allowing individuals to make a truly informed choice. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

41. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

## II. Defendants Violate the Biometric Information Privacy Act.

42. By the time BIPA passed through the Illinois Legislature in mid-2008, most companies who had experimented with using individuals' biometric data stopped doing so.

43. However, Defendants continue to collect, store, use and disseminate their employees' biometric data in violation of BIPA.

44. Specifically, when employees are hired, Defendants require them to have their fingerprints scanned to enroll them in its employee database(s) so that they can access keys to restricted areas.

45. Defendants use a key dispenser that requires employees to use their fingerprint as a means of authentication. In accordance with Defendants' policy, all of their employees who are granted access to restricted areas are required to use their fingerprints to gain access.

46. Upon information and belief, Defendants have failed to inform all of their employees that they disclose or disclosed their fingerprint data to third parties, including third parties which host the biometric data in their data centers, and failed to inform their employees of the purposes and for which they collect their sensitive biometric data.

47. Furthermore, Defendants have failed to provide employees with a written, publicly available policy identifying their retention schedule and guidelines for permanently destroying employees' biometric data when the initial purpose for collecting or obtaining their biometric data is no longer relevant, as required by BIPA.

48. The Pay by Touch bankruptcy that catalyzed the passage of BIPA, as well as the recent data breaches, highlight why such conduct – where individuals are aware that they are providing a fingerprint, but not aware of to whom or for what purposes they are doing so – is dangerous. This bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers, such as a fingerprint, who exactly is collecting their biometric data, where it will be transmitted and for what purposes, and for how long. Defendants disregard these obligations and their employees' statutory rights and instead unlawfully collect, store, use and disseminate their biometric identifiers and information, without ever receiving a fully-compliant informed written consent required by BIPA.

49. Remarkably, Defendants have created the same situation that Pay by Touch did by assembling a database of biometric data through fingerprint scanners, but failed to comply with the law specifically designed to protect individuals whose biometrics are collected in these circumstances. Defendants disregard these obligations and Illinois employees' statutory rights and instead unlawfully collect, store, use, and disseminate employees' biometric identifiers and information without ever receiving the individual's fully-compliant informed written consent required by BIPA.

50. Plaintiff and other similarly situated employees are not told what might happen to their biometric data if and when Defendants merge with another company, or worse, if and when

Defendants' businesses fold, or when the other third parties that have received their employees' biometric data's businesses fold.

51. Since Defendants neither publishes a BIPA-mandated data retention policy nor fully discloses the purposes for its collection and use of biometric data, employees have no idea the extent to whom Defendants sell, disclose, re-disclose, or otherwise disseminate their biometric data. Moreover, Plaintiff and others similarly situated are not told to whom Defendants currently disclose their biometric data, or what might happen to their biometric data in the event of a merger or a bankruptcy.

52. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

53. By and through the actions detailed above, Defendants disregard Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

## III. Plaintiff Ronnie Alquero's Experience

54. Plaintiff Ronnie Alquero worked for Defendants as a Food and Beverage Shift Manager from May 2008 until April 2019.

55. Defendants required Plaintiff to scan his fingerprint so it could be used as an authentication method to gain access to a key dispenser needed to enter restricted areas.

56. Defendants subsequently stored Plaintiff's fingerprint data in their employee database(s).

57. Defendants required Plaintiff to scan his fingerprint each time he needed to obtain a key to enter restricted areas.

58. Upon information and belief, Plaintiff has never been informed of the specific limited purposes or length of time for which Defendants collect, store, use and/or disseminate his biometric data.

59. Upon information and belief, Plaintiff has never been informed of any biometric data retention policy developed by Defendants, nor has he ever been informed of whether Defendants will ever permanently delete his biometric data.

60. Upon information and belief, Plaintiff has never been provided with nor ever signed a written release allowing Defendants to collect, store, use or disseminate his biometric data.

61. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendants' multiple violations of BIPA as alleged herein.

62. No amount of time or money can compensate Plaintiff if his biometric data is compromised by the lax procedures through which Defendants captured, stored, used, and disseminated his and other similarly-situated individuals' biometric data. Moreover, Plaintiff would not have provided his biometric data to Defendants if he had known that it would retain such information for an indefinite period of time without his consent.

63. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act"). Nonetheless, Plaintiff is aggrieved because he suffers an injury-in-fact based on Defendants' violations of his legal rights. Defendants have intentionally interfered with Plaintiff's right to possess and control his own sensitive biometric data. Additionally, Plaintiff

suffered an invasion of a legally protected interest when Defendants secured his personal and private biometric data at a time when they had no right to do so, a gross invasion of his right to privacy. BIPA protects employees like Plaintiff Alquero from this precise conduct. Defendants had no lawful right to secure this data or share it with third parties absent a specific legislative license to do so.

64. Plaintiff's biometric information is economically valuable, and such value will increase as the commercialization of biometrics continues to grow. As such, Plaintiff has not been sufficiently compensated by Defendants for their retention and use of his and other similarly-situated employees' biometric data. Plaintiff would not have agreed to work for Defendants for the compensation he receives if he had known that Defendants would retain his biometric data indefinitely.

65. Plaintiff also suffered an informational injury because Defendants have failed to provide him with information to which he was entitled by statute. Through BIPA, the Illinois legislature has created a right: an employee's right to receive certain information prior to an employer securing their highly personal, private and proprietary biometric data; and an injury – not receiving this extremely critical information.

66. Plaintiff also suffered an injury in fact because Defendants have improperly disseminated his biometric identifiers and/or biometric information to third parties that hosted the biometric data in their data centers, in violation of BIPA.

67. Pursuant to 740 ILCS § 14/15(b), Plaintiff was entitled to receive certain information prior to Defendants securing his biometric data; namely, information advising him of the specific limited purpose(s) and length of time for which Defendants collect, store, use and disseminate his private biometric data; information regarding Defendants' biometric retention

policy; and a written release allowing Defendants to collect, store, use, and disseminate his private biometric data. By depriving Plaintiff of this information, Defendants injured him. *Public Citizen v. U.S. Department of Justice*, 491 U.S. 440, 449 (1989); *Federal Election Commission v. Akins*, 524 U.S. 11 (1998).

68. Plaintiff has plausibly inferred actual and ongoing harm in the form of monetary damages for the value of the collection and retention of his biometric data; in the form of monetary damages by not obtaining additional compensation as a result of being denied access to material information about Defendants' policies and practices; in the form of the unauthorized disclosure of his confidential biometric data to third parties; in the form of interference with his right to control and possess his confidential biometric data; and, in the form of the continuous and ongoing exposure to substantial and irreversible loss of privacy.

69. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, he seeks statutory damages under BIPA as compensation for the injuries caused by Defendants. *Rosenbach*, 2019 IL 123186, ¶ 40.

**CLASS ALLEGATIONS**

70. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS § 5/2-801, Plaintiff brings claims on his own behalf and as a representative of all other similarly-situated individuals pursuant to BIPA, 740 ILCS § 14/1, *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed.

71. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it ***first*** (1) informs the individual in writing that a biometric identifier or biometric information is being collected or

stored; (2) informs the individual in writing of the specific purpose(s) and length of time 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.

72. Plaintiff seeks class certification under the Illinois Code of Civil Procedure, 735 ILCS § 5/2-801, for the following class of similarly-situated individuals under BIPA:

> All individuals working in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by Defendants during the applicable statutory period.

73. This action is properly maintained as a class action under 735 ILCS § 5/2-801 because:

A. The class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the class;

C. Plaintiff's claims are typical of the claims of the class; and,

D. Plaintiff will fairly and adequately protect the interests of the class.

**Numerosity**

74. The total number of putative class members exceeds one hundred (100) individuals. The exact number of class members can easily be determined from Defendants' records.

**Commonality**

75. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendants' failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether Defendants collected, captured or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

B. Whether Defendants properly informed Plaintiff and the Class of their purposes for collecting, using, storing and disseminating their biometric

identifiers or biometric information;

C. Whether Defendants obtained a written release (as defined in 740 ILCS § 14/10) to collect, use, store and disseminate Plaintiff's and the Class's biometric identifiers or biometric information;

D. Whether Defendants have disclosed or re-disclosed Plaintiff's and the Class's biometric identifiers or biometric information;

E. Whether Defendants have sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometric identifiers or biometric information;

F. Whether Defendants developed 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 three years of its last interaction with the individual, whichever occurs first;

G. Whether Defendants comply with any such written policy (if one exists);

H. Whether Defendants used Plaintiff's and the Class's fingerprints to identify them;

I. Whether Defendants' violations of BIPA have raised a material risk that Plaintiff's and the Class's biometric data will be unlawfully accessed by third parties;

J. Whether the violations of BIPA were committed negligently; and

K. Whether the violations of BIPA were committed intentionally and/or recklessly.

76. Plaintiff anticipates that Defendants will raise defenses that are common to the class.

**Adequacy**

77. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiff and class members. Plaintiff, moreover, has retained experienced counsel who are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

**Typicality**

78. The claims asserted by Plaintiff are typical of the class members he seeks to represent. Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

79. Upon information and belief, there are no other class members who have an interest individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim and the difficulties involved in bringing individual litigation against one's employer. However, if any such class member should become known, he or she can "opt out" of this action pursuant to 735 ILCS § 5/2-801.

**Predominance and Superiority**

80. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

81. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent

and varying adjudications, establish incompatible standards of conduct for Defendants and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

## FIRST CAUSE OF ACTION

### Violation of 740 ILCS § 14/15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

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

83. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 14/15(a).

84. Defendants fail to comply with these BIPA mandates.

85. Defendant Eldorado Resorts, Inc. is a corporation that does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

86. Defendant Elgin Riverboat Resort – Riverboat Casino, d/b/a Grand Victoria Riverboat Casino is an Illinois general partnership that does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

87. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by Defendants (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

88. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

89. Defendants failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

90. Upon information and belief, Defendants lack retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and have not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

91. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) 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 for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

## SECOND CAUSE OF ACTION

### Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

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

93. BIPA requires companies to obtain informed written consent from individuals before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity

to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] ***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) (emphasis added).

94. On information and belief, Defendants have failed to comply with these BIPA mandates.

95. Defendant Eldorado Resorts, Inc. is a corporation that does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

96. Defendant Elgin Riverboat Resort – Riverboat Casino, d/b/a Grand Victoria Riverboat Casino is an Illinois general partnership that does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

97. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by Defendants (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

98. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

99. Defendants systematically and automatically collect, use, store and disseminate Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining a fully-complaint written release required by 740 ILCS § 14/15(b)(3).

100. Defendants failed to inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, stored, used, and disseminated. Defendants additionally failed to inform Plaintiff and the Class in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS § 14/15(b)(1)-(2).

101. By collecting, storing, using and disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendants violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq*.

102. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) 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 for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

## THIRD CAUSE OF ACTION
### Violation of 740 ILCS § 14/15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

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

104. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS § 14/15(d)(1).

105. Defendants have failed to comply with this BIPA mandate.

106. Defendant Eldorado Resorts, Inc. is a corporation that does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

107. Defendant Elgin Riverboat Resort – Riverboat Casino, d/b/a Grand Victoria Riverboat Casino is an Illinois general partnership that does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

108. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by Defendants (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

109. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

110. On information and belief, Defendants systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS § 14/15(d)(1).

111. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendants violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq.*

112. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) 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 for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for <u>each</u> intentional and/or reckless violation of BIPA pursuant to 740 ILCS §

14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

**PRAYER FOR RELIEF**

Wherefore, Plaintiff Ronnie Alquero 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 Ronnie Alquero as Class Representative, and appointing Stephan Zouras, LLP, as Class Counsel;

B. Declaring that Defendants' actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 for *each* intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS § 14/20(1);

D. Declaring that Defendants' actions, as set forth above, were intentional or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendants to collect, store, use, destroy and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3);

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

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

**JURY TRIAL**

Plaintiff demands a trial by jury for all issues so triable.

Dated: August 20, 2019

Respectfully Submitted,

*/s/ Ryan F. Stephan*

Ryan F. Stephan
Teresa M. Becvar

Stephan Zouras, LLP
100 North Riverside Plaza
Suite 2150
Chicago, Illinois 60606
(312) 233-1550
(312) 233-1560 *f*
rstephan@stephanzouras.com
tbecvar@stephanzouras.com
Firm ID: 43734

*Attorneys for the Plaintiff and the Putative Class*

**CERTIFICATE OF SERVICE**

I, the attorney, hereby certify that on August 20, 2019, I electronically filed the attached with the Clerk of the Court using the electronic filing system which will send such filing to all attorneys of record.

*/s/ Ryan F. Stephan*