

unloading, track maintenance, inspection or repair. Railserve is a member company of The Marmon Group.

4. Marmon Railroad is limited liability company in Illinois doing business in Illinois providing locomotives repair services and overhauling rail locomotives. Marmon Railroad is a member of Marmon Group.

5. Marmon Holdings is a global industrial corporation registered in Delaware and doing business in Illinois. Marmon Holdings organization includes Marmon's Rail Group, that groups companies, including Railserve and Marmon Railroad, that design, build, repair and lease for the rail business. Marmon Holdings is the parent company of all other Defendants named herein.

6. Defendants are private entities related in the railroad service business and form a group under the BIPA.

7. Defendants are a private entity, as defined under BIPA 740 ILCS 14/10 which means any individual, partnership, corporation, limited liability company, association, or other group, however organized.

8. During relevant periods, upon information and belief, Defendants employed in excess of 65 employees and staffers in Illinois.

Jurisdiction and Venue

9. The Court possesses general subject matter jurisdiction over the state law the state law BIPA claims. Jurisdiction is proper under 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendants are doing business within this State and because Plaintiff's and the Class's claims arise out of Defendants unlawful in-state actions, as Defendants captured, collected, stored, and used Plaintiff's biometric identifiers and/or biometric information in this State.

10. Venue is proper in the circuit court of Cook County because Plaintiff resides in Cook County and Defendants employed Plaintiff to work at their site in Bedford Park, Illinois.

The Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq and Public Policies

11. BIPA defines a “biometric identifier” as any personal feature that is unique to an individual, including fingerprints and palm scans. “Biometric information” is any information based on a biometric identifier, regardless of how it is converted or stored. 740 ILCS § 14/10. Collectively, biometric identifiers and biometric information are known as “biometrics”.

12. Biometric technology allows companies to reduce timekeeping fraud. Unfortunately, along with the increased utility of biometric technology, so too come grave privacy risks associated with the unauthorized or malicious dissemination of this information.

13. The risk of harm is greatly magnified when biometrics are obtained in violation of reasonable regulations designed to protect individuals’ irreplaceable information. The permanent and irreplaceable nature of one’s biometrics makes the illegal collection of the same a significant public problem with far-reaching consequences, including irreversible identity theft.

14. Recognizing the irreversible harm presented by allowing the unregulated collection and use of biometrics, Illinois passed the BIPA, a statute addressing the collection, use, retention, possession, and dissemination of biometrics by private entities, such as Defendants.

15. Under BIPA, a biometric system, such as Defendants’ system, is legal if, and only if, Defendants first:

(1) informs the person whose biometrics are to be collected in writing that biometric identifiers or biometric information will be collected or stored;

(2) informs the person whose biometrics are to be collected in writing of the specific purpose and the length of term for which such biometric identifiers or biometric information is being collected, stored and used;

(3) receives a written release from the person whose biometrics are to be collected, allowing the capture and collection of their biometric identifiers or biometric information; and

(4) publishes publicly available retention guidelines for permanently destroying biometric identifiers and biometric information. 740 ILCS 14/15(a).

16. Compliance with BIPA is straightforward and may be accomplished through a single, signed sheet of paper. BIPA's requirements bestow a right to privacy in biometrics and a right to make an informed decision when electing whether to provide or withhold biometrics.

17. The Illinois Legislature has found that "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, even sensitive information like Social Security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to each individual and therefore, once compromised, such individual has no recourse, is at a heightened risk for identity theft in, and is likely to withdraw from biometric facilitated transactions." 740 ILCS 14/5. The risk is compounded when a person's biometric information is also associated with his/her Social Security Number and potentially other relevant financial information or personal identifiable information. The gravity of the unresolvable problems created in the event of a data breach is so severe that the unlawful collection of such information constitutes actual harm.

18. 740 ILCS 14/15 provides in relevant part:

"Retention; collection; disclosure; destruction.

(a) 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. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No private entity may collect, 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 or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
- (2) informs the subject or the subject's legally authorized representative 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.

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

- (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
- (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
- (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance;
or
- (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction."

19. Plaintiff brings this action for damages and other remedies resulting from the actions of Defendants in capturing, storing, using, and disseminating his biometrics, and those other individuals throughout the state of Illinois, without informed written consent, and without informing them through a publicly available policy of how and when the subject biometrics would be stored or disposed of, in direct violation of the Illinois BIPA.

Common Facts

20. Within the five years prior to initiating this action, Plaintiff worked at Defendants' sites in Bedford Park, Illinois.

21. Within the five years prior to initiating this action, Defendants used biometric scanning technology to monitor and track its employees' and other staffers, including Plaintiff's, time.

22. Defendants' biometric timekeeping system extracts biometric information from individuals, such as fingerprints or portions thereof, and subsequently using the same for authentication and timekeeping purposes. The system includes the dissemination of biometrics to third parties, such as data storage vendors and payroll services. The biometrics are stored and repeatedly used each time a worker "clocks in" or "out" on the job.

23. As part of his work at Defendants' facilities, Plaintiff was required to scan his fingerprints and/or other biometrics into Defendants' biometric timekeeping device each time he needed to "clock-in" and "clock-out". Defendants was aware that Plaintiff and other class members would be required to utilize the biometric timekeeping technology.

24. As a result of Plaintiff's use of Defendants' timekeeping system, Defendants took possession and control of Plaintiff's biometric information.

25. Upon information and belief, after Defendants took possession and control of Plaintiff's biometric information, Defendants disclosed such information to third parties including its third-party payment processor(s).

26. Plaintiff relied on Defendants to not only provide a lawful and legally compliant system, but to also disclose all material information regarding the technology and system, including retention, destruction, and dissemination policies.

27. Defendants were aware, or reckless in failing to be aware, that its employees and staffers would be subject to its biometric technology. Defendants were aware that its biometric

technology would be capturing, collecting, utilizing, and/or disseminating the biometrics of Plaintiff and the Class members.

28. Defendants' biometric technology allows for and resulted in the dissemination of Plaintiff and other Class member's biometrics to third parties, including vendors for timekeeping, data storage, and payroll purposes.

29. Prior to taking possession of Plaintiff's biometrics through its biometric technology, Defendants did not inform Plaintiff in writing that his biometrics were being collected, stored, used, or disseminated, or publish any policy specifically about the collection, retention, use, deletion, or dissemination of biometrics.

30. Prior to taking possession of Plaintiff's biometrics through its biometric technology, Defendants did not obtain a written consent from Plaintiff relating to the collection, use, storage, or dissemination of his biometrics.

31. Prior to taking possession of Plaintiff's biometrics, Plaintiff never provided to Defendants a written consent relating to the collection, use, storage, or dissemination of his biometrics.

32. Prior to taking possession of Plaintiff's biometrics, Defendants did not make publicly available any written policy as to a biometric retention schedule and guidelines for permanently destroying the collected biometrics.

33. Prior to taking possession of Plaintiff's biometrics, Defendants did not have a publicly available policy of informing individuals, including Plaintiff, of what happens to their biometrics after they are captured, whether the information is disseminated to a third party and, if so, which third party, and what would happen to the data if Defendants was to be acquired or file bankruptcy.

34. Prior to taking possession of Plaintiff's biometrics, Defendants did not obtain consent from Plaintiff for the dissemination of his biometrics to third parties.

35. To this day, Plaintiff is unaware of the status of his biometrics obtained and possessed by Defendants.

36. Defendants have not informed Plaintiff whether it still retains his biometrics, and if they do, for how long they intend to retain such information without his consent.

37. Within the five years prior to initiating this action Defendants captured, stored, used, and/or disseminated the biometrics of Plaintiff and other Class members without their informed written consent as required by law.

38. To the extent Defendants are still retaining Plaintiff's biometrics, such retention is unlawful. Plaintiff would not have provided his biometric data to Defendants or utilized its biometric timekeeping technology had he known the same would remain with Defendants for an indefinite period or subject to unauthorized disclosure.

Class Allegations

39. Plaintiff brings this action on behalf of himself and all similarly-situated individuals pursuant to 735 ILCS § 5/2-801. Plaintiff seeks to represent certain class(es) defined as follows:

Class 1: All persons whose biometrics were possessed, captured, collected, stored, used, transmitted, or disseminated by or on behalf of Railserve, Inc., Marmon Holdings, Inc. and Marmon Railroad Services LLC or its technology while Defendants did not maintain a compliant, publicly-available written policy related to retention and destruction of such biometrics, from May 8, 2019 through class certification, within the State of Illinois.

Class 2: All persons whose biometrics were possessed, captured, collected, stored, used, transmitted, or disseminated by or on behalf of Railserve, Inc., Marmon Holdings, Inc. and Marmon Railroad Services LLC or its technology without

Defendants first obtaining a compliant written consent, from May 8, 2019, through class certification, within the State of Illinois.

Class 3: All persons whose biometrics were disclosed by or on behalf of Railserve, Inc., Marmon Holdings, Inc. and Marmon Railroad Services LLC or its technology to third parties, without consent or authorization, from May 8, 2019, through class certification, within the State of Illinois.

The prospective members of all three classes above are referred to cumulatively as the “Class” or “Class Members” herein.

40. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendants; and any immediate family member of such officers or directors.

41. Upon information and belief, there are over sixty-five members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiff, the members can be easily identified through Defendants’ personnel records.

42. Plaintiff’s claims are typical of the claims of the members of the Class he seeks to represent, because the factual and legal bases of Defendants’ liability to Plaintiff and the other members are the same, and because Defendants’ conduct has resulted in similar injuries to Plaintiff and to the Class. As alleged herein, Plaintiff and the Class have all suffered damages as a result of Defendants’ BIPA violations.

43. There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members. Common questions for the Class include, but are not limited to, the following:

- a. Whether Defendants' timekeeping technology and associated conduct is subject to BIPA;
- b. Whether Defendants made available to the public a written policy that establishes a retention schedule and guidelines for destroying biometrics;
- c. Whether Defendants obtained a written release from the Class before capturing, collecting, or otherwise obtaining their biometrics;
- d. Whether Defendants provided a written disclosure that explains the specific purposes, and the length of time, for which biometrics were being collected, stored and used before taking such biometrics;
- e. Whether Defendants' conduct violates BIPA;
- f. Whether Defendants' conduct is negligent;
- g. Whether Defendants' violations of the BIPA are willful or reckless; and
- h. Whether Plaintiff and the Class are entitled to damages and injunctive relief;
- i. Whether Defendants provided a written disclosure that explains the specific purposes, and the length of time, for which biometrics were being collected, stored and used before taking such biometrics.

44. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

45. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class he seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Class.

46. Defendants has acted and failed to act on grounds generally applicable to the Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

47. BIPA requires private entities, such as Defendants, to obtain informed written consent from individuals before acquiring their biometric information. Specifically, BIPA makes it unlawful to “collect, capture, purchase, receive through trade, or otherwise obtain a person's or 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 for which a biometric identifier or biometric information is being captured, 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).

48. BIPA requires that private entities in possession of biometric identifiers and/or biometric information establish and maintain a publicly available retention policy. Entities which possess biometric identifiers or information must (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric information (entities may not retain biometric information longer than three years after the last interaction with the individual); and (ii) adhere to the publicly posted retention and deletion schedule.

49. Plaintiff and the other Class members have had their “biometric identifiers”, namely their fingerprints, possessed, collected, captured, received or otherwise obtained by Defendants and/or its technology. Plaintiff and the other Class members’ biometric identifiers were also used to identify them, and therefore constitute “biometric information” as defined by BIPA. 740 ILCS 14/10

50. Each instance Plaintiff and the other Class members had their fingerprints scanned into Defendants' biometric devices, Defendants and/or its technology possessed, captured, collected, stored, and/or used Plaintiffs and the other Class members' biometric identifiers or biometric information without valid consent and without complying with and, thus, in violation of BIPA.

51. Defendants' practice with respect to possessing, capturing, collecting, storing, and using biometrics fails to comply with applicable BIPA requirements:

a. Defendants failed to inform Plaintiff and the members of the Class in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);

b. Defendants failed to inform Plaintiff and Class in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

c. Defendants failed to inform Plaintiff and the Class in writing the specific length of term their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

d. Defendants failed to obtain a written release, as required by 740 ILCS 14/15(b)(3);

e. Defendants failed to provide a publicly available retention schedule detailing the length of time for which the biometrics are stored and/or guidelines for permanently destroying the biometrics they store, as required by 740 ILCS 14/15(a); and/or

f. Defendants failed to obtain informed consent to disclose or disseminate Plaintiff's and the Class's biometrics, as required by 740 ILCS 14/15(d)(1).

52. By designing and operating an employee timekeeping system which uses biometrics that was devoid of the privacy protections required by BIPA, Defendants profited from Plaintiff's and the Class members' biometric identifiers and biometric information in violation of 740 ILCS 14/15(c).

53. Defendants knew, or were reckless in not knowing, that the biometric systems they were using, selling, maintaining, and/or servicing would be subject to the provisions of BIPA yet failed to comply with the statute.

54. By capturing, collecting, storing, using, and disseminating Plaintiffs and the Class members' biometrics as described herein, Defendants denied Plaintiff and the Class their right to statutorily-required information and violated their respective rights to biometric information privacy, as set forth in the BIPA.

Damages and Relief

55. Had Defendants informed Plaintiff that he was not being provided with the required information regarding his biometrics and the biometric timekeeping program it was providing as required by law, or that the biometric technology it was providing was not legally compliant, he would not have worked in the subject employment conditions or agreed to provide his biometrics without additional compensation.

56. Had Defendants provided Plaintiff with all required disclosures, he at least would have been able to make an informed decision concerning material facts of the work environment, including whether the rate of pay and opportunity cost justified participating in the biometric timekeeping program.

57. Plaintiff's and the Class's biometrics are economically valuable and such value will increase as the commercialization of biometrics continues to grow. Defendants' repeated use of Plaintiff's biometrics does and will continue to confer a benefit on Defendants for which Plaintiff was not sufficiently compensated.

58. By failing to comply with BIPA, Defendants has violated Plaintiffs substantive state rights to biometric information privacy.

59. Defendants' violations of the BIPA, as set forth herein, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendants negligently failed to comply with BIPA.

60. The BIPA provides for statutory damages of \$5,000 for each willful and/or reckless violation of the BIPA and, alternatively, damages of \$1,000 for each negligent violation of the BIPA. 740 ILCS 14/20(1).

61. On behalf of himself and the proposed Class defined below, Plaintiff seeks an injunction requiring Defendants to comply with BIPA, as well as an award of statutory damages to the Class members and common law monetary damages to be determined at trial, together with costs and reasonable attorneys' fees.

Count 1 - Plaintiff and the Class - Violation of BIPA - Section 15(a)

62. Plaintiff reincorporates Paragraphs 1 through 61, as if set forth in full herein for ¶ 62.

63. BIPA Section 15(a) 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. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines."

64. Within the last five years prior to Plaintiff initiating this action, Defendants obtained and possessed Plaintiff's and the Class's biometric identifiers or biometric information.

65. Despite possessing Plaintiff's and the Class's biometric identifiers or biometric information, Defendants failed to 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.

66. As a direct and proximate result, Defendants violated Section 15(a) of BIPA.

Wherefore, Plaintiff, on behalf of himself and the proposed Class, prays for:

- a. the certification of the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;
- b. a declaration that Defendants' actions violate BIPA;
- c. an award of injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendants to comply with the BIPA requirements for the capture and collection of biometrics, as well as requiring Defendants to comply with the written retention policy requirements of 740 ILCS 14/15(a);
- d. an award of statutory damages of \$5,000 for each willful and/or reckless violation of BIPA, pursuant to 740 ILCS 14/20(1);
- e. an award of statutory damages of \$1,000 for each negligent violation of BIPA, pursuant to 740 ILCS 14/20(3);
- f. an award of reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3); and/or
- g. Grant such additional or alternative relief as this Honorable Court deems just and proper.

Count 2 - Plaintiff and the Class - Violation of BIPA - Section 15(b)

67. Plaintiff reincorporates Paragraphs 1 through 61, as if set forth in full herein for ¶ 67.

68. BIPA Section 15(b) provides:

“(b) No private entity may collect, 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 or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
- (2) informs the subject or the subject's legally authorized representative 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.”

69. Prior to taking possession, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining Plaintiff's and the Class's biometric identifier or biometric information,

Defendants did not inform Plaintiff or the Class or their legally authorized representative(s) in writing that a biometric identifier or biometric information was being collected or stored.

70. Prior to taking possession, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining Plaintiff's and the Class's biometric identifier or biometric information, Defendants did not inform Plaintiff or the Class or their legally authorized representative(s) in writing of the specific purpose and length of term for which their biometric identifier or biometric information was being collected, stored, and used.

71. Prior to taking possession, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining Plaintiff's and the Class's biometric identifier or biometric information, Defendants did not receive a written release executed by Plaintiff or the Class or their legally authorized representative(s).

72. As a direct and proximate result, Defendants violated Section 15(b) of BIPA.

Wherefore, Plaintiff, on behalf of himself and the proposed Class, prays for:

- a. the certification of the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;
- b. a declaration that Defendants' actions violate BIPA;
- c. an award of injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendants to comply with the BIPA requirements for the capture and collection of biometrics, as well as requiring Defendants to comply with the written retention policy requirements of 740 ILCS 14/15(a);
- d. an award of statutory damages of \$5,000 for each willful and/or reckless violation of BIPA, pursuant to 740 ILCS 14/20(1);
- e. an award of statutory damages of \$1,000 for each negligent violation of BIPA, pursuant to 740 ILCS 14/20(3);
- f. an award of reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3); and/or
- g. Grant such additional or alternative relief as this Honorable Court deems just and proper.

Count 3 - Plaintiff and the Class - Violation of BIPA - Section 15(d)

73. Plaintiff reincorporates Paragraphs 1 through 61, as if set forth in full herein for ¶ 73.

74. BIPA Section 15(d) provides:

“(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

- (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
- (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
- (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
- (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.”

75. Upon information and belief, Defendants disclosed Plaintiff's and the Class's biometric identifiers or biometric information to third parties, including Defendants' third party payroll processor(s)

76. Plaintiff and the Class did not consent to Defendants' disclosure or redisclosure of their biometric identifiers or biometric information. Defendants did not inform Plaintiff or the Class or their legally authorized representative(s) in writing that a biometric identifier or biometric information was being collected or stored.

77. Neither the Plaintiff nor the Class requested or authorized the disclosure or redisclosure of their biometric identifiers or the biometric information to any third parties.

78. Defendants' disclosure of Plaintiff's and the Class's biometric identifiers or biometric information to third parties was not required by State or federal law or municipal ordinance.

79. Defendants' disclosure of Plaintiff's and the Class's biometric identifiers or biometric information to third parties was not required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

80. As a direct and proximate result, Defendants violated Section 15(d) of BIPA.

Wherefore, Plaintiff, on behalf of himself and the proposed Class, prays for:

- a. the certification of the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;
- b. a declaration that Defendants' actions violate BIPA;
- c. an award of injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendants to comply with the BIPA requirements for the capture and collection of biometrics, as well as requiring Defendants to comply with the written retention policy requirements of 740 ILCS 14/15(a);
- d. an award of statutory damages of \$5,000 for each willful and/or reckless violation of BIPA, pursuant to 740 ILCS 14/20(1);
- e. an award of statutory damages of \$1,000 for each negligent violation of BIPA, pursuant to 740 ILCS 14/20(3);
- f. an award of reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3); and/or
- g. Grant such additional or alternative relief as this Honorable Court deems just and proper.

/s/ James M. Dore

Justicia Laboral LLC - Firm ID 61282
Daniel I. Schlade (ARDC No. 6273008)
James M. Dore (ARDC# 6296265) (Cook Cty. #45224)
Attorneys for Plaintiffs
6232 N. Pulaski Rd., #300; Chicago, IL 60646
P: 773-415-4898
E: jdore@justicialaboral.com
dschlade@justicialaboral.com

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Railserve, Marmon Holdings Hit with Privacy Class Action in Illinois Over Employee Fingerprint Scanning](#)
