IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS
PEORIA DIVISION

JOHN KARARO, individually, and on behalf of all other Illinois citizens similarly situated, Plaintiffs, v. OLD DOMINION FREIGHT LINE INC., Defendant.	)	Case No. Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiff JOHN KARARO, as a proposed class representative, by and through attorney James C. Vlahakis, asserts the following claims against Defendant OLD DOMINION FREIGHT LINE INC., pursuant to the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*.

I. Parties, Jurisdiction and Venue

1. Plaintiff JOHN KARARO ("Plaintiff") is a citizen of Illinois and resides in this judicial district.

2. Defendant MACLELLAN INTEGRATED SERVICES, INC. ("Defendant") conducts business in the State of Illinois and within this judicial district.

3. Plaintiff is an employee of Defendant.

4. Plaintiff works for Defendant in a facility located in Normal, Illinois.

5. Defendant is Virginia corporation and maintains its corporate office in Thomasville, North Carolina.

6. Defendant's registered agent is CT Corporation System, 208 S. LaSalle St. Suite 814, Chicago IL 60604.

7. This Court has personal jurisdiction over Defendant because it maintains a business location in this judicial district and Defendant has violated BIPA through its business practices conducted within this judicial district.

8. As detailed below, this Court has subject matter jurisdiction over Plaintiff's individual claims on the basis of diversity jurisdiction. See, 28 U.S.C. § 1332.

9. BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

10. As detailed below, during Plaintiff's employment with Defendant, Defendant utilized a time clock system that required Plaintiff and other employees to scan, upload and/or use at least one form of a unique "biometric identifier" in order allow Plaintiff and other employees to log in and out of Defendant's time clock system.

11. Defendant's Kronos time clock system required Plaintiff and other employees to scan, upload and/or use their unique fingerprint in order to use Defendant's time clock.

12. Defendant's time clock system utilized, collected, stored and otherwise obtained the unique biometric identifiers of Plaintiff and other similarly situated employees in violation of the prohibition set forth by BIPA.

13. "[D]istrict courts shall have original jurisdiction of all civil actions where the matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs, and is between — (1) citizens of different States[.]" 28 U.S.C. § 1332.

14. As alleged above, Plaintiff is citizen of the State of Illinois and Defendant is a foreign corporation with its headquarters and principal place of business located outside the State of Illinois.

15. Plaintiff could recover $75,000.00 in statutory damages by using Defendant's time clock system a minimum of seventy-five (75) times.

16. 28 U.S.C. § 1391(b)(2) provides that "[a] civil action may be brought in – (2) a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred[.]"

17. Venue is proper in this judicial district, a substantial part of the events or omissions giving rise to Defendant's violations of BIPA took place within this district.

18. Venue is also proper in this judicial district because Plaintiff is a citizen of the State of Illinois and Plaintiff seeks to vindicate Plaintiff's rights (and the rights of putative class members) as provided by BIPA.

19. Further, venue is proper in this judicial district because Defendant's putative class members are all citizens of the State of Illinois.

II. The Biometric Privacy Act

20. BIPA was enacted in 2008 for the purpose of addressing a "very serious need for protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Session No. 276.

21. BIPA's express Legislative Findings provide as follows:

> (c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. 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.
>
> (d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.
>
> (e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.
>
> (f) The full ramifications of biometric technology are not fully known.
>
> (g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

740 ILCS 14/5.

22. The Illinois Supreme Court has recognized that BIPA "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach v. Six Flags Ent. Corp.*, 432 Ill. Dec. 654, 129 N.E.3d 1197, 1206 (Ill. 2019).

23. A private entity's failure to comply with BIPA "is no mere 'technicality'", as the Illinois Supreme Court has explained:

> The duties imposed on private entities by section 15 of the Act (740 ILCS 14/15 (West 2016)) regarding the collection, retention, disclosure, and destruction of a person's or customer's biometric identifiers or biometric information define the contours of that statutory right. Accordingly, when a private entity fails to comply with one of section 15's requirements, that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach.
>
> * * *
>
> The Act vests in individuals and customers the right to control their biometric information by requiring notice *before* collection and giving them the power to say no by withholding consent. . . . When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, "the right of the individual to maintain his or her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized." This is no mere "technicality." The injury is real and significant.

Id. (emphasis supplied).

24. BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

25. BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10.

26. BIPA prohibits private entities from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's biometric information unless the private entity: (1) informs that person in writing that identifiers and information will

be collected and/or stored; (2) informs the person in writing of the specific purpose and length for which the identifiers or information is being collected, stored or used; (3) receives a written release from the person for the collection of that data; and (4) publishes publicly available written retention schedules and guidelines for permanently destroying said data. *See* 740 ILCS 14/15(a) and (b).

27. As detailed below, within the past five years (the "Relevant Time Period"), Defendant required Plaintiff and other current and former employees (hereafter, "putative class members") to use a time clock system to track their hours worked.

28. The time clock system utilized by Defendant required Plaintiff and putative class members to input, use, upload and/or store one of their unique "biometric identifiers" in order to in an out of the time clock system.

29. Upon information and belief, the time clock system utilized by Defendant used, captured, collected and/or stored the "biometric identifiers" of Plaintiff and putative class members.

30. The time clock system utilized by Defendant required Defendant to obtain written consent from Plaintiff and putative class members *before* it was able to acquire or otherwise capture the "biometric identifiers" of Plaintiff and putative class members.

31. Section 20(1) of BIPA provides that "[a] prevailing party may recover for each violation: ... (1) against a private entity negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater[.]" 740 ILCS 14/20(1).

32. Section 20(2) of BIPA provides that "[a] prevailing party may recover for each violation: ... (a) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater[.]" 740 ILCS 14/20(2).

III. CAFA Jurisdiction

33. The Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), provides federal jurisdiction over putative class action claims if the following conditions are met:

> (2) The district courts shall have original jurisdiction of any civil action in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and is a class action in which—
>
> (A) any member of a class of plaintiffs is a citizen of a State different from any defendant[.]

28 U.S.C. § 1332(d)(2).

34. Section 1332(d)(6) of CAFA provides that "[i]n any class action, the claims of the individual class members shall be aggregated to determine whether the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs."

35. Plaintiff satisfies Section 1332(d)(2)(A) because Defendant and the putative members are citizens of different states.

36. Upon information and belief, during the Relevant Time Period, more than 100 putative class members utilized Defendant's time clock system in violation of BIPA. See, 28 U.S.C. § 1332(d)(5)(B)

37. The requirement of Section 1332(d)(2) is satisfied where 5,001 individual violations of BIPA (involving 100 or more putative class members) would exceed $5,000,000 in damages.

38. Within the past week, Defendant has attempted to secure BIPA consent forms from employees by offering to pay them $500.

Count I – Asserting Violations of Section 15(a) of BIPA

39. Plaintiff reasserts and incorporates the above Paragraphs as if fully set forth above.

40. Biometric identifiers are unlike other unique identifiers that are used to access finances or other sensitive information.

41. Biometric identifiers and biometric information are biologically unique to the individual.

42. Biometric identifiers and biometric information cannot be easily changed.

43. Public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers.

44. Section 15(a) of BIPA states that 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[.]"

45. In particular, Section 15(a) required Defendant to publish "to the public", "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."

46. Defendant does not maintain a public policy which identifies its data retention and destruction protocols.

47. "The BIPA requirement to implement data retention and destruction protocols protects a person's biometric privacy just as concretely as the statute's informed-consent regime." *Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1155 (7th Cir. 2020).

48. Because Defendant does not maintain a public policy which identifies its data retention and destruction protocols, Plaintiff reasonably believes that Defendant

does not destroy "biometric identifiers" or "biometric information" after "the initial purpose for collecting or obtaining such identifiers or information has been satisfied" as required by 740 ILCS 14/15(a).

49. Upon information and belief, Defendant does not destroy "biometric identifiers" or "biometric information" "within 3 years of the individual's last interaction with the private entity" as required by 740 ILCS 14/15(a).

50. Defendant's violations of Section 15(a) of BIPA have resulted in the *unlawful retention* of Plaintiff and proposed class members' "biometric identifiers" and/or "biometric information[.]"

51. The " unlawful retention of biometric data inflicts a privacy injury in the same sense that an unlawful collection does." *Fox*, 980 F.3d at 1154-55.

52. As a result of Defendant's conduct, Plaintiff and putative class members to suffer harm, and they are entitled to liquidated damages as provided by 740 ILCS 14/20(1)-(2).

53. The proposed Class is comprised of all current and former employees of Defendant (working in the State of Illinois) who had their "biometric information" and/or "biometric identifiers" collected, captured, or otherwise obtained by Defendant in violation of Section 15(a) of BIPA.[1]

54. The proposed Class is ascertainable from Defendant's records.

55. Common questions of law and fact exist.

56. The claims in this Count are typical of the claims of putative class members.

[1] This definition is not a so-called "fail safe" class definition. *See, e.g., Heard v. Becton, Dickenson & Co.*, 534 F.Supp.3d 831, 848-49 (N.D. Ill. 2021).

57. The defenses that Defendant may assert against Plaintiff are typical of the types of defenses that Defendant may assert against putative class members.

58. Plaintiff will fairly and adequately protect the interests of the putative class members because Plaintiff seeks to assert statutory rights afforded by BIPA and seeks to obtain declaratory, injunctive and monetary relief for all class members.

59. The proposed Class should be certified to avoid inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for the party opposing the class.

60. The proposed Class should be certified to avoid adjudications with respect to individual class members that, as a practical matter, would be dispositive of the interests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests.

61. The proposed Class should be certified because Defendant has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

62. The proposed Class should be certified because questions of law or fact common to class members predominate over any questions affecting only individual members, and because a class action is superior to other available methods for fairly and efficiently adjudicating the present controversy.

63. Proposed class counsel will fairly and adequately protect the interest of the putative class members. *See, e.g., Molinari v. Fin. Asset Mgmt. Sys., Inc.*, 2021 U.S. Dist. LEXIS 235401, *3 (N.D. Ill. Nov. 22, 2021) (appointing attorney James C. Vlahakis as provisional class counsel in putative class action involving the Fair Debt Collection Practices Act and the Telephone Consumer Protection Act, with final approval being granted by Dkt. 134). *See also, In re: Apple Inc. Device Performance Litigation*, 18-md-

02827, 2023 U.S. Dist. LEXIS 27892, 2023 WL 2090981 (Feb. 17, 2023) (granting final approval of a $310 million dollar settlement fund where Plaintiff's counsel represented two dozen class representatives).

WHEREFORE, Plaintiff respectfully requests that this Honorable Court provide Plaintiff and putative class members with the following relief:

a. Declaring that Defendant violated Section 15(a) of BIPA;
b. Requiring Defendant to publish a public policy which identifies its data retention and destruction protocols;
c. Requiring Defendant to destroy "biometric identifiers" or "biometric information" after "the initial purpose for collecting or obtaining such identifiers or information has been satisfied";
d. Awarding liquidated damages for negligent violations of Section 15(a);
e. Awarding liquidated damages for intentional and/or reckless violations of Section 15(a);
f. Awarding reasonable attorney's fees and costs;
g. Enjoining Defendant from further violations of Section 15(a); and
h. Certifying the proposed Class set forth above.

Count II – Asserting Violations of Section 15(b) of BIPA

64. Plaintiff reasserts and incorporates the above Paragraphs as if fully set forth above.

65. Section 15(b) of BIPA states that "[n]o 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" takes the following actions:

> (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.

66. BIPA defines "[w]ritten release" as "informed written consent." 740 ILCS 14/10.

67. Defendant violated Section 15(b) of BIPA because it collected Plaintiff's "biometric identifiers" and/or "biometric information" without first obtaining Plaintiff's informed written consent.

68. Defendant also violated Section 15(b) of BIPA because it collected the "biometric identifiers" and/or "biometric information" of putative class members without first obtaining their informed written consent.

69. Defendant violated of Section 15(b)(1) of BIPA by failing to inform Plaintiff in writing that it was storing and/or collecting Plaintiff's "biometric identifiers" or "biometric information." 740 ILCS 14/15(b)(1).

70. Defendant violated of Section 15(b)(1) of BIPA by failing to inform putative class members in writing that it was storing and/or collecting their "biometric identifiers" or "biometric information." 740 ILCS 14/15(b)(1).

71. Defendant violated of Section 15(b)(2) of BIPA by failing to inform Plaintiff in writing of the specific purpose and length of term for which Plaintiff's "biometric identifiers" and/or "biometric information" was "being collected, stored, and used." 740 ILCS 14/15(b)(2).

72. Defendant violated of Section 15(b)(2) of BIPA by failing to inform putative class members in writing of the specific purpose and length of term for which their "biometric identifiers" and/or "biometric information" was "being collected, stored, and used." 740 ILCS 14/15(b)(2).

73. Defendant violated of Section 15(b)(3) of BIPA by failing to obtain a written release from Plaintiff before Defendant collected Plaintiff's "biometric identifiers" and/or "biometric information." 740 ILCS 14/15(b)(3).

74. Defendant violated of Section 15(b)(3) of BIPA by failing to obtain a written release from putative class members before Defendant collected their "biometric identifiers" and/or "biometric information." 740 ILCS 14/15(b)(3).

75. As explained above, Defendant collected, used and/or stored Plaintiff's and class members' "biometric identifiers" and/or "biometric information" in violation of the prohibitions and requirements set forth by Section 15(b) of BIPA.

76. As explained above, Defendant did not obtain the informed written consent of Plaintiff and putative class members to collect, use, modify and/or store their "biometric identifiers" and/or "biometric information."

77. Plaintiff and putative class members have suffered damages in the form of liquidated damages as provided by 740 ILCS 14/20(1)-(2).

78. The proposed Class is defined as all current and former employees of Defendant in the State of Illinois who had their "biometric information" and/or "biometric identifiers" collected, captured and otherwise obtained by Defendant in violation of Section 15(b) of BIPA. [2]

79. The proposed Class is ascertainable from Defendant's records.

80. Common questions of law and fact exist.

81. The claims in this Court which assert that Defendant violated Section 15(b) of BIPA by requiring Plaintiff to use a time clock system that collected, captured, and otherwise obtained Plaintiff's "biometric information" and/or "biometric identifiers" *without* Plaintiff's express written consent - is typical of the claims of putative class members.

[2] This definition is not a so-called "fail safe" class definition. *See, e.g., Heard v. Becton, Dickenson & Co.*, 534 F.Supp.3d 831, 848-49 (N.D. Ill. 2021).

82. Plaintiff will fairly and adequately protect the interests of the putative class members because Plaintiff seeks to assert statutory rights afforded by BIPA and seeks to obtain declaratory, injunctive and monetary relief for all class members.

83. The proposed Class should be certified to avoid inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for the party opposing the class.

84. The proposed Class should be certified to avoid adjudications with respect to individual class members that, as a practical matter, would be dispositive of the interests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests.

85. The proposed Class should be certified because Defendant has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

86. The proposed Class should be certified because questions of law or fact common to class members predominate over any questions affecting only individual members, and because a class action is superior to other available methods for fairly and efficiently adjudicating the present controversy.

87. Proposed class counsel will fairly and adequately protect the interest of the putative class members. *See, e.g., Molinari v. Fin. Asset Mgmt. Sys., Inc.*, 2021 U.S. Dist. LEXIS 235401, *3 (N.D. Ill. Nov. 22, 2021) (appointing attorney James C. Vlahakis as provisional class counsel in putative class action involving the Fair Debt Collection Practices Act and the Telephone Consumer Protection Act, with final approval being granted by Dkt. 134). *See also, In re: Apple Inc. Device Performance Litigation*, 18-md-02827, 2023 U.S. Dist. LEXIS 27892, 2023 WL 2090981 (Feb. 17, 2023) (granting final

approval of a $310 million dollar settlement fund where Plaintiff's counsel represented two dozen class representatives).

WHEREFORE, Plaintiff respectfully requests that this Honorable Court provide Plaintiff and putative class members with the following relief:

a. Declaring that Defendant violated Section 15(b)(1) of BIPA;
b. Declaring that Defendant violated Section 15(b)(2) of BIPA;
c. Declaring that Defendant violated Section 15(b)(3) of BIPA;
d. Requiring Defendant to publish a public policy which identifies its data retention and destruction protocols;
e. Requiring Defendant to destroy "biometric identifiers" or "biometric information" after "the initial purpose for collecting or obtaining such identifiers or information has been satisfied";
f. Awarding liquidated damages for negligent violations of Section 15(a);
g. Awarding liquidated damages for intentional and/or reckless violations of Section 15(a);
h. Awarding reasonable attorney's fees and costs;
i. Enjoining Defendant from further violations of Section 15(a); and
j. Certifying the proposed Class set forth above.

Jury Demand

Plaintiff demands a jury trial.

/s/ James C. Vlahakis

James C. Vlahakis
Vlahakis Law Group LLC
20 N. Clark Street, Suite 3300
Chicago IL 60602
312-766-0511 (office)
312-648-6127 (direct)
jamesv@vlahakislaw.com

Counsel for Plaintiff and the putative class members

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Old Dominion Employee Fingerprint Scans Violate Illinois Privacy Law, Class Action Claims

---