IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS
EAST ST. LOUIS

HEATHER MCCLAINE, on behalf of herself and all other persons similarly situated, known and unknown,	)	
Plaintiff,	)	Case No.: 3:23-cv-01168-DWD
v.	)	Judge David W. Dugan
DX ENTERPRISES, INC. f/k/a DX ENTERPRISES, LLC d/b/a DXE, d/b/a GCQA, LLC,	)	Jury Trial Demanded
Defendant.	)	

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff, Heather McClaine ("Plaintiff"), on behalf of herself and all other persons similarly situated, known and unknown, files this First Amended Class Action Complaint ("Complaint")[1] as a matter of right, pursuant to Federal Rule of Civil Procedure 15(a)(1)(B), against DX Enterprises, Inc., f/k/a DX Enterprises, LLC, d/b/a DXE, d/b/a GCQA, LLC ("DXE" or "Defendant"), for violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, and states:

INTRODUCTION

1. Defendant, DX Enterprises, Inc. is a privately owned foreign corporation that is a full-service staffing and logistics company, located in Princeton, Indiana in Gibson County.

2. Defendant, upon information and belief, operates under the assumed business names of both DXE and GCQA (both DXE and Gibson County Quality Assurance LLC are listed on the

[1] This matter was originally filed as a class action complaint in the Circuit Court of Lawrence County, case no. 2023-LA-1, but was subsequently removed by Defendant pursuant to 28 U.S.C. § 1441(a) and (b), and Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). Dkt. # 1, pg. 3-4.

Indiana Secretary of State's website as the assumed business names for the entity DX Enterprises, Inc., both operate under the same business ID (2012020100247), Defendant's LinkedIn page lists the company name as, "DXE Staffing/GCQA LLC", and Defendant's Facebook Page lists both the names "DXE & GCQA LLC").

3. Plaintiff, Heather McClaine, is a former employee of Defendant.

4. Plaintiff was employed by Defendant at a Toyota Factory in Lawrenceville, Illinois from approximately March 2019 through September 2019 and again February or March 2021.

5. Defendant required Plaintiff and other employees to use a biometric "fingerprint" time clock system to record their time worked.

6. Unlike an employee identification number or employee identification card, fingerprints are *unique* and *permanent* identifiers.

7. By requiring employees to scan their fingerprints to record their time, instead of identification numbers or badges only, Defendant ensured that one employee could not clock in for another.

8. Thus, DXE received labor management benefits from using a biometric timeclock.

9. Defendant achieved financial benefits from using a biometric time clock.

10. Likewise, Defendant placed employees at risk based on the use of employees' biometric identifiers, after they had been made to use the biometric timeclock(s) in question and without complying with the statutes addressed herein.

11. As is set forth in greater detail below, Defendant violated BIPA, in several respects, by: (1) improperly capturing and/or collecting the biometric identifiers of the Plaintiff and the class that she seeks to represent; (2) failing to provide adequate written notice, informing the Plaintiff and the class that she seeks to represent of the same; (3) failing to obtain written releases from the Plaintiff and the class she seeks to represent; and (4) improperly disclosing and/or disseminating the biometric

identifiers of the Plaintiff and the class she seeks to represent. 740 Ill. Comp. Stat. Ann. 14/15.

THE PARTIES

12. Plaintiff is an individual and a citizen of Illinois.

13. Defendant, DXE, is a foreign corporation, located in Princeton, Indiana in Gibson County residing and doing business in Illinois.

14. DXE's principal office is in Princeton, Indiana.

JURISDICTION

15. This Court has jurisdiction pursuant to 28 U.S.C. § 1441(a) and (b), and Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d).

SUMMARY OF CLAIMS

16. Defendant required Plaintiff and other employees to utilize the biometric time clock system, in order to (a) verify the identity of a particular employee; and (b) maintain a system of record of various information including but not limited to the employees' hours worked and a host of other beneficial use cases, as discussed in greater detail below.

17. Plaintiff, and all others similarly situated, were required to place their fingers onto a scanning device that scanned, recorded, and/or otherwise captured images of their fingerprints.

18. These images were scanned, recorded, and/or otherwise captured, each and every time Plaintiff and other employees commenced and/or ended work in the facility.

19. These images were, likewise, recorded, and/or otherwise captured, each and every time Plaintiff and other employees to a break from their work in the facility.

20. The data pertaining to these images was stored on devices, including but not limited to the local memory of the scanning device mentioned in ¶¶ 16-17, hereinafter referred to as the "biometric timeclock."

21. The data pertaining to these images was also stored on other devices, including but

not limited to:

a. devices owned, operated, leased, and/or licensed by Defendant, including but not limited to any manner of usufruct transaction; and

b. devices owned, operated, leased, licensed, and/or otherwise accessible to Defendant, as a result of a software license or contractual relationships with a third party.

22. By virtue of requiring the Plaintiff and other employees to utilize the biometric time clock by scanning their fingerprints, Defendant collected and, subsequently, possessed Plaintiff and other employees' biometric identifiers, to wit, their fingerprints and/or the biometric identifiers derived from their scanning of their fingerprints.

23. Defendant advertises on its website that it provides "Daily Attendance/Turnover/Disciplinary Reporting to Customer," and "Thorough Attendance Reporting, addressing absences with TMs immediately."

24. Likewise, and upon information and belief, Defendant utilized the biometric data collected from Plaintiff and the Class to provide daily attendance, turnover, and disciplinary reporting to companies for which it provided staffing services.

25. Defendant's use of Plaintiff and the Class's biometric identifiers for, in relevant part, daily attendance, turnover, and disciplinary reporting demonstrates it collected, possessed, and disseminated these biometric identifiers.

26. Unlike an employee identification number or employee identification card, fingerprints are *unique* and *permanent* identifiers.

27. By requiring employees to scan their fingerprints to record their time, instead of identification numbers or badges only, this ensured that one employee could not clock in for another.

28. Thus, in addition to multiple other labor management benefits, DXE achieved a labor

management benefit from using a biometric time clock mechanism.

29. The machine and supporting software utilized by Defendant, ensures that Plaintiff, and all others similarly situated, could only verify their attendance and timeliness using its biometric timekeeping device.

30. Defendant, through its use of the biometric timeclocks collected and possessed the biometric identifiers, to wit, the fingerprints of the Plaintiff and the Class she seeks to represent.

31. In enacting BIPA, the Illinois legislature recognized that biologically unique identifiers, like fingerprints, can never be changed when compromised, and thus subject a victim of identity theft to heightened risk of loss.

32. As a result, Illinois restricted private entities, like Defendant, from collecting, storing, using, or transferring a person's biometric identifiers and information without adhering to strict informed-consent procedures established by BIPA.

33. Plaintiff used Defendant's biometric timeclock, thereby having her fingerprints collected, possessed, and, ultimately, disclosed by Defendant, when she clocked in and out of work each day and throughout her employment with Defendant.

34. By DXE requiring Plaintiff to scan her biometric identifiers, to wit, her fingerprints, Defendant captured and/or collected, and, subsequently, possessed Plaintiff's biometric identifiers.

35. Defendant collected and/or captured, stored, used, and transferred the unique biometric fingerprint identifiers, or information derived from those identifiers, of Plaintiff and others similarly situated without following the detailed requirements of BIPA.

36. As a result, Defendant violated BIPA and compromised the privacy and security of the biometric identifiers and information of Plaintiff and other similarly situated employees.

REQUIREMENTS OF THE BIOMETRIC INFORMATION PRIVACY ACT

37. In enacting BIPA, the Illinois legislature recognized that the full ramifications of

biometric technology are not yet fully known and so the public will benefit from "regulations on the collection, use, safeguarding, handling, storage retention, and description of biometric identifiers and information." 740 ILCS 14/5(f)-(g).

38. BIPA prohibits a "private entity" from capturing or collecting biometric identifiers or information from an individual unless that private entity first obtains the individual's written consent or employment-related release authorizing the private entity to capture or collect an individual's biometric identifiers and/or biometric information. 740 ILCS 14/15(b)(3).

39. Relatedly, BIPA prohibits a private entity from capturing or collecting biometric identifiers or information from an individual unless that private entity first informs the individual, in writing, of the following: (a) that the private entity is collecting biometric identifiers or information, (b) the purpose of such collection, and (c) the length of time the private entity will retain the biometric identifiers or information. 740 ILCS 14/15(b)(1)-(2).

BACKGROUND FACTS (BIOMETRIC PRIVACY ACT ALLEGATIONS)

40. When Plaintiff and other employees scanned their fingerprints in Defendant's biometric time clock mechanism, Defendant, and potentially others, captured and/or collected, and stored their fingerprints, or personal identifying information derived from their fingerprints.

41. When Plaintiff and other employees scanned their fingerprints into the biometric time clock mechanism, DXE, likewise, possessed Plaintiff's and other employees' fingerprints and/or personal identifying information derived from their fingerprints.

42. Defendant, subsequently, stored Plaintiff's fingerprint data, in the form of a unique, user-specific template, in their systems, the locations of which are not yet known.

43. Defendant's use of Plaintiff's and other employees' biometric identifiers, to wit, fingerprints and/or personal identifying information derived from their fingerprints, to prevent one employee for clocking in for another, and to track their hours worked demonstrates, further,

Defendant's possession and/or control over their biometric identifiers.

44. When Plaintiff scanned her fingerprint into the biometric time clock mechanism, DXE disclosed her fingerprint – or personal identifying information derived from her fingerprint – to amongst potentially as of yet identified parties.

45. Defendant improperly disclosed the biometric timeclock users' fingerprint data to other, currently unknown, third parties, including, but not limited to third parties that host biometric data in their data center(s).

46. Upon information and belief, this included one or more third-party timekeeping vendors and/or to Toyota as part of the staffing agreement between Defendant and Toyota.

47. Before requiring Plaintiff, and the class of people she seeks to represent, to use a biometric time clock, Defendant never provided Plaintiff any materials, including in writing, stating that it was collecting, retaining, or disclosing her fingerprint or personal identifying information derived from her fingerprint.

48. Prior to requiring Plaintiff to use the biometric time clock mechanism, DXE never obtained Plaintiff's written consent or a written release, as a condition of employment, authorizing the collection, storage, dissemination, or use of her fingerprint or personal identifying information derived from Plaintiff's fingerprint.

49. Defendant violated Plaintiff's privacy by capturing or collecting her unique biometric identifiers and information and sharing those identifiers and information with various other parties without her consent.

50. In addition, BIPA prohibits a private entity from possessing biometric identifiers or information unless it creates and follows a written policy, made available to the public, establishing a retention schedule and destruction guidelines for its possession of biometric identifiers and information. 740 ILCS 14/15(a).

51. Prior to collecting and/or otherwise capturing Plaintiff's biometric identifiers through use of its biometric technology, Defendant failed to make publicly available any written policy as to a biometric identifier retention schedule, or guidelines for permanently destroying the collected biometric identifiers.

52. Upon information and belief, Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly situated individuals' biometric data and have not and will not destroy their biometric data as required by BIPA. Accordingly, Defendant continues to possess and/or otherwise retain control over Plaintiff's and other employees' biometric identifiers, to wit, their fingerprints and/or personal identifying information derived from their fingerprints.

53. Finally, BIPA prohibits private entities from disclosing or otherwise disseminating biometric identifiers or information without first obtaining an individual's consent for that disclosure or dissemination, unless the disclosure or dissemination was (a) in furtherance of an authorized financial transaction, (b) authorized by law, or (c) pursuant to a valid warrant or subpoena. 740 ILCS 14/15(d).

54. Defendant failed to obtain consent from the Plaintiff, and the class she seeks to represent, before disclosing or otherwise disseminating their biometric identifiers.

BIOMETRIC INFORMATION PRIVACY ACT CLASS ACTION ALLEGATIONS

55. Plaintiff seeks to represent a putative class, the "Class" pursuant to 735 ILCS 5/2-802.

56. The Class consists of:

> All employees of DX Enterprises, Inc., f/k/a DX Enterprises, LLC, d/b/a DXE, d/b/a GCQA, LLC ("DXE"), including but not limited to employees hired by DXE and assigned to the Toyota manufacturing facility, who scanned their fingerprints and/or other biometric identifiers into the biometric timeclock mechanism, or whose biometric identifiers as defined under 740 ILCS 14/10 were utilized in any manner by DXE, between February 2018 and the present without first executing a written release.

57. The Class's claims all stem from the same or substantially similar conduct, as they were all subject to the same allegedly illegal practices of DXE's failure to adhere to the requirements of

BIPA.

58. The Class includes more than 50 members.

59. Defendant's own notice of removal, and the affidavit filed in support of the same, admit that at least 579 individuals are members of the Class. Dkt. # 1, pg. 5; 1-2, pg. 2.

60. Indeed, by the admission of William Boss, Defendant's President, approximately 579 individuals used the biometric timeclock at issue, and would have used it multiple times. Dkt. 1-2, pg. 2.

61. The issues involved in this lawsuit present common questions of law and fact, including:

a. Whether DXE required members of the Class to scan their fingerprints to clock in and out during shifts;

b. Whether Defendant collected the Class "biometric identifiers" or "biometric information" under BIPA;

c. Whether Defendant properly informed Plaintiff and the Class of its purposes for collecting, obtaining, using, storing and disseminating their biometric identifiers or biometric information;

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

e. Whether Defendant has disclosed or re-disclosed Plaintiff's and the Class's biometric identifiers or biometric information;

f. Whether Defendant has sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometric identifiers or biometric information;

g. Whether Defendant 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;

h. Whether Defendant complies with any such written policy (if one exists);

i. Whether Defendant used Plaintiff's and the Class's fingerprints to identify them;

j. Whether Defendant's violations of BIPA have raised a material risk that Plaintiff's biometric data will be unlawfully accessed by third parties;

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

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

62. Plaintiff also anticipates that Defendant will raises defenses that are common to the class.

63. These common questions of law and fact predominate over variations that may exist between members of the Class, if any.

64. 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.

65. 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 Defendant 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.

66. Plaintiff, the members of the Class, and Defendant have a commonality of interest in the subject matter of the lawsuit and the remedy sought.

67. If individual actions were required to be brought by each member of either the Class injured or affected, the result would be a multiplicity of actions, creating a hardship to the Class, to the Court, and to Defendant.

68. Accordingly, a class action is an appropriate method for the fair and efficient adjudication of this lawsuit and distribution of the common funds to which the Classes are entitled.

69. The books and records of Defendant are material to Plaintiff's case as they disclose how and when Plaintiff and the Class had their fingerprints scanned in Defendant's biometric time clock system and what information Defendant provided Plaintiff and the Class about the collection, retention, use, and dissemination of their biometric identifiers and information.

70. Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Plaintiff retained counsel is experienced in complex class action litigation.

DEFENDANT'S CONDUCT WAS INTENTIONAL OR RECKLESS

71. BIPA provides that any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation: (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater; or (2) 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.

72. Defendant's actions, in violating BIPA, demonstrated courses of action, which showed a knowing risk or conscious disregard that their conduct would harm the Plaintiff, the Class, and/or an utter indifference to, or conscious disregard for the biometric privacy rights of the Plaintiff and the class he seeks to represent, as well as the safety and security of their biometric identifiers.

73. Despite the fact that BIPA had been in existence since 2008, and by extension, set the minimum notice, consent, and security requirements for collection of biometric identifiers in Illinois, DXE failed to independently investigate or take precautions to ensure its compliance with BIPA.

74. Defendant advertises that it provides a robust interview process and "Customer Approved Screening Process," which includes:

a. Background checks – hire to Customer criteria;

b. Drug screens prior to hiring – regular random screening;

c. [Online] testing available most industries (over 1000 tests available); and

d. In House Orientation (OSHA focused, and can include customer-specific information or training).

75. The fact that Defendant provides the foregoing services demonstrates its awareness of its requirement to comply with certain employment laws and regulations.

76. Notwithstanding those representations, Defendant knew or should have known that its biometric timeclock and its practices for collecting and/or capturing, possessing, storing, destroying, and disseminating Plaintiff and the Class's biometric identifiers were legally inadequate, and did not comply with BIPA.

77. However, and upon information and belief, despite utilizing the biometric data collected from the Plaintiff and the Class to provide this service, Defendant failed to investigate whether its use of said data complied with BIPA.

78. Upon information and belief, DXE undertook no precautions to ensure its compliance with BIPA, did not establish a data retention, storage, or destruction policy, and left the sufficiency of its security measures for protecting Plaintiff and the Class's biometric identifiers to chance.

79. Defendant's failure to investigate its policies' legality or compliance with BIPA demonstrates an utter indifference to, or conscious disregard for the biometric privacy rights of the Plaintiff and the Class she seeks to represent, as well as the safety and security of their biometric identifiers.

80. Accordingly, Defendant's violations of BIPA were reckless or intentional.

DEFENDANT'S CONDUCT FAILED TO MEET DATA SECURITY STANDARD OF CARE

81. BIPA also sets forth, in relevant part, that a private entity that collects or possesses biometric identifiers or biometric information meet a certain industry/data security standard of care with respect to its handling of those biometric identifiers or biometric information.

82. BIPA provides, specifically:

> (e) A private entity in possession of a biometric identifier or biometric information shall:
>
> > (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
> >
> > (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

740 Ill. Comp. Stat. Ann. 14/15.

83. As set forth in ¶¶ 71-80, Defendant was aware of certain privacy and regulatory requirements attendant to its industry, but failed to investigate similar obligations with respect to employees' data privacy, and, by extension, ensuring compliance with protecting or safeguarding employees' biometric identifiers and/or biometric information.

84. Upon information and belief, the standard of care in the staffing and logistics industry requires compliance with BIPA.

85. Defendant failed to meet this industry standard of care by virtue of the following acts:

a. Failing to obtain Plaintiff and the Class's written consent before capturing or collecting her unique biometric identifiers and information and sharing those identifiers and information with various other parties;

b. Failing to create and follow a written policy, made available to the public, establishing a retention schedule and destruction guidelines for its possession of biometric identifiers and information before collecting Plaintiff and the Class's unique biometric identifiers and information; and

c. Disclosing or otherwise disseminating biometric identifiers or information without first obtaining an individual's consent for that disclosure or dissemination, as the disclosure or dissemination was (a) not in furtherance of an authorized financial transaction; (b) authorized by law; or (c) pursuant to a valid warrant or subpoena.

86. As a result of the foregoing, Defendant violated BIPA's requirement that it protect employee data pursuant to the standard of care in its industry.

COUNT I
Violation of the Biometric Information Privacy Act (740 ILCS 14/15(b))
(Class Action)

87. Plaintiff realleges and incorporates the previous allegations of this First Amended Class Action Complaint.

88. DXE is a "private entity" under BIPA. 740 ILCS 14/10.

89. Plaintiff's and the Class's fingerprints qualify as "biometric identifier[s]" as defined by BIPA. 740 ILCS 14/10.

90. DXE has "biometric information" from Plaintiff and the Class through its acquisition

and retention of personal identifying information based on Plaintiff's and the Class's fingerprints.

91. DXE violated BIPA by capturing or collecting Plaintiff's and the Class's fingerprints and personal identifying information based on their fingerprints without first informing them in writing that DXE was doing so.

92. DXE violated BIPA by capturing or collecting Plaintiff's and the Class's fingerprints and personal identifying information based on their fingerprints without first informing them in writing of the purpose of DXE doing so and the length of time DXE would store and use Plaintiff's and the Class's biometric identifiers and/or biometric information.

93. Defendant violated BIPA by capturing or collecting Plaintiff's and the Class's fingerprints and personal identifying information based on their fingerprints without first obtaining their written consent or other release authorizing the Defendant to capture or collect Plaintiff's and the Class's biometric identifiers and/or biometric information.

94. Unlike other companies doing business in Illinois, DXE failed to take notice and follow the requirements of BIPA, even though the law was enacted in 2008, and numerous articles and court filings about the law's requirements were published before the Defendant committed the legal violations alleged in this Complaint.

95. DXE's violation of BIPA was reckless or intentional or, in the alternative, negligent.

WHEREFORE, Plaintiff and the Class pray for a judgment against DXE as follows:

A. Awarding liquidated or actual monetary damages, whichever is higher, to Plaintiff and Class for each violation of BIPA as provided by 740 ILCS 14/20(1)-(2);

B. Enjoining DXE from committing further violations of BIPA as authorized by 740 ILCS 14/20(4);

C. Awarding Plaintiff's reasonable attorneys' fees and costs incurred in filing and prosecuting this action as provided by 740 ILCS 14/20(3); and

D. Such other and further relief as this Court deems appropriate and just as provided by 740 ILCS 14/20(4).

COUNT II
Violation of the Biometric Information Privacy Act (740 ILCS 14/15(a))
(Class Action)

96. Plaintiff realleges and incorporates the previous allegations of this First Amended Class Action Complaint.

97. DXE is a "private entity" under BIPA. 740 ILCS 14/10.

98. Plaintiff's and the Class's fingerprints qualify as "biometric identifier[s]" as defined by BIPA. 740 ILCS 14/10.

99. DXE has "biometric information" from Plaintiff and the Class through its acquisition and retention of personal identifying information based on Plaintiff's and the Class's fingerprints.

100. DXE violated BIPA by possessing Plaintiff's and the Class's fingerprints and personal identifying information based on their fingerprints without creating and following a written policy, made available to the public, establishing a retention schedule and destruction guidelines for its possession of biometric information derived from Plaintiff's and the Class's fingerprints.

101. Unlike other Illinois companies, DXE failed to take notice and follow the requirements of BIPA even though the law was enacted in 2008 and numerous articles and court filings about the law's requirements were published before DXE committed the legal violations alleged in this Complaint.

102. As a result, DXE's violations of BIPA were reckless or intentional, or, in the alternative, negligent.

WHEREFORE, Plaintiff and the Class pray for a judgment against DXE as follows:

A. Awarding liquidated or actual monetary damages, whichever is higher, to Plaintiff and the Class for each violation of BIPA as provided by 740 ILCS 14/20(1)-(2);

B. Enjoining DXE from committing further violations of BIPA as authorized by 740 ILCS 14/20(4);

C. Awarding Plaintiff's reasonable attorneys' fees and costs incurred in filing and prosecuting this action as provided by 740 ILCS 14/20(3); and

D. Such other and further relief as this Court deems appropriate and just as provided by 740 ILCS 14/20(4).

COUNT III
Violation of the Biometric Information Privacy Act (740 ILCS 14/15(d))
(Class Action)

103. Plaintiff realleges and incorporates the previous allegations of this First Amended Class Action Complaint.

104. DXE is a "private entity" under BIPA. 740 ILCS 14/10.

105. Plaintiff's and the Class's fingerprints qualify as "biometric identifier[s]" as defined by BIPA. 740 ILCS 14/10.

106. DXE has "biometric information" from Plaintiff, the Class, and the Class through its acquisition and retention of personal identifying information based on Plaintiff's and the Class's fingerprints.

107. DXE violated BIPA by disclosing or otherwise disseminating Plaintiff's and the Class's fingerprints and information based on their fingerprints to third parties, including but not limited to Defendant's time-keeping vendor, without first obtaining their consent for that disclosure or dissemination.

108. Unlike other Illinois companies, DXE failed to take notice and follow the requirements of BIPA even though the law was enacted in 2008 and numerous articles and court filings about the law's requirements were published before DXE committed the legal violations alleged in this Complaint.

109. As a result, DXE's violations of BIPA were reckless or intentional or, in the alternative, negligent.

WHEREFORE, Plaintiff and the Class pray for a judgment against DXE as follows:

A. Awarding liquidated or actual monetary damages, whichever is higher, to Plaintiff and the Class for each violation of BIPA as provided by 740 ILCS 14/20(1)-(2);

B. Enjoining DXE from committing further violations of BIPA as authorized by 740 ILCS 14/20(4);

C. Awarding Plaintiff's reasonable attorneys' fees and costs incurred in filing and prosecuting this action as provided by 740 ILCS 14/20(3); and

D. Such other and further relief as this Court deems appropriate and just as provided by 740 ILCS 14/20(4).

COUNT IV
Violation of the Biometric Information Privacy Act (740 ILCS 14/15(e))
(Class Action)

110. Plaintiff realleges and incorporates the previous allegations of this First Amended Class Action Complaint.

111. DXE is a "private entity" under BIPA. 740 ILCS 14/10.

112. Plaintiff's and the Class's fingerprints qualify as "biometric identifier[s]" as defined by BIPA. 740 ILCS 14/10.

113. DXE has "biometric information" from Plaintiff, the Class, and the Class through its acquisition and retention of personal identifying information based on Plaintiff's and the Class's fingerprints.

114. As set forth more fully in ¶¶ 71-85, DXE failed to store, transmit, and protect from disclosure the Plaintiff's and the Class's biometric identifiers and information, using the reasonable standard of care within DXE's industry, and failed to store, transmit, and protect said information in the same or more protective manner in which DXE stores, transmits, and protects its other confidential and sensitive information.

115. As a result of DXE's actions described herein DXE violated the Illinois Biometric Information Privacy Act.

116. Unlike other Illinois companies, DXE failed to take notice and follow the requirements of BIPA even though the law was enacted in 2008 and numerous articles and court filings about the law's requirements were published before DXE committed the legal violations alleged

in this Complaint.

117. As a result, DXE's violations of BIPA were reckless or intentional or, in the alternative, negligent.

WHEREFORE, Plaintiff and the Class pray for a judgment against DXE as follows:

A. Awarding liquidated or actual monetary damages, whichever is higher, to Plaintiff and the Class for each violation of BIPA as provided by 740 ILCS 14/20(1)-(2);

B. Enjoining DXE from committing further violations of BIPA as authorized by 740 ILCS 14/20(4);

C. Awarding Plaintiff's reasonable attorneys' fees and costs incurred in filing and prosecuting this action as provided by 740 ILCS 14/20(3); and

D. Such other and further relief as this Court deems appropriate and just as provided by 740 ILCS 14/20(4).

Respectfully submitted,

Dated: May 24, 2023

/s/ Max P. Barack
One of Plaintiff's Attorneys

The Garfinkel Group, LLC
Max P. Barack (ARDC No.: 6312302)
Haskell Garfinkel (ARDC No.: 6274971)
701 N. Milwaukee Ave
The CIVITAS
Chicago, Illinois 60642
Telephone: (312) 736-7991
max@garfinkelgroup.com
haskell@garfinkelgroup.com

Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that, on May 24, 2023, a copy of the foregoing First Amended Complaint was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt.

/s/ Max P. Barack
Attorney for Plaintiff

ClassAction.org