YES / (NO)

EXHIBITS

CASE NO. 2019 CH 9096

DATE: 8/6/19

CASE TYPE: CLASS ACTION

PAGE COUNT: 10

CASE NOTE

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

KENYATTA NICHOLS, on behalf of herself and all other persons similarly situated, known and unknown,	)	Case No. 2019CH09096
Plaintiff,	)	Judge
v.	)	Hearing Date: 12/4/2019 10:00 AM - 10:00 AM Courtroom Number: 2410 Location: District 1 Court Cook County, IL
WHOLE FOODS MARKET GROUP, INC.	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Kenyatta Nichols ("Plaintiff"), files this Class Action Complaint against Whole Foods Market Group, Inc., d/b/a Whole Foods ("Defendant") for violations of the Illinois Biometric Information Privacy Act.

SUMMARY OF CLAIMS

1. Defendant is a natural and organic grocer operating Whole Foods stores throughout Illinois.

2. Plaintiff was employed at Defendant's store located at 7245 Lake Street in River Forest, Illinois 60305.

3. Plaintiff was employed by Defendant as an hourly employee in its prepared foods and deli section from approximately April 2017 to July 2017.

4. Defendant required employees to use a biometric time clock system to record their time worked.

5. Defendant required Plaintiff and other employees to scan their fingerprints in Defendant's biometric time clock each time they started and finished working, including punching

in and out for lunch breaks.

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

7. By requiring employees to use 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, there's no question that Defendant benefited from using a biometric time clock.

9. But there's equally no question that Defendant placed employees at risk by using their biometric identifiers to "punch the clock."

10. In enacting the Biometric Information Privacy Act, 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.

11. 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 the Biometric Information Privacy Act.

12. Defendant collected, 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 the Biometric Information Privacy Act.

13. As a result, Defendant violated the Biometric Information Privacy Act and compromised the privacy and security of the biometric identifiers and information of Plaintiff and other similarly-situated employees.

JURISDICTION AND VENUE

14. This Court has personal jurisdiction over Defendant because, during the relevant time period, Defendant did business in Illinois, was registered to do business in Illinois, and committed the statutory violations alleged in this Class Action Complaint in Illinois.

15. Cook County is an appropriate venue for this litigation because Defendant has grocery stores in Cook County, does business there, and the events giving rise to this lawsuit happened there.

THE PARTIES

16. Plaintiff is an individual who lives in Cook County Illinois.

17. Defendant is a Delaware corporation.

18. Defendant's principal place of business is in Austin, Texas.

REQUIREMENTS OF THE BIOMETRIC INFORMATION PRIVACY ACT

19. In enacting the Biometric Information Privacy Act, 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).

20. The Biometric Information Privacy Act 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).

21. Relatedly, the Biometric Information Privacy Act 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)(b).

22. In addition, the Biometric Information Privacy Act prohibits a private entity from possessing biometric identifiers or information unless it first creates 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).

23. Finally, the Biometric Information Privacy Act prohibits a private entity 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).

BACKGROUND FACTS

24. When Plaintiff scanned her fingerprint in Defendant's biometric time clock, Defendant captured and stored Plaintiff's fingerprint, or a representation derived from Plaintiff's fingerprint.

25. When Plaintiff scanned her fingerprint in Defendant's biometric time clock, her fingerprint – or a representation derived from her fingerprint – was disseminated and disclosed to Defendant's time-keeping vendor.

26. Defendant never provided Plaintiff any written materials stating that it was collecting, retaining, or disseminating her fingerprint or a representation derived from her fingerprint.

27. Defendant never obtained Plaintiff's written consent, or release as a condition of employment, authorizing the collection, storage, dissemination, or use her fingerprint or a representation derived from Plaintiff's fingerprint.

28. Defendant violated Plaintiff's privacy by capturing or collecting her unique biometric identifiers and information, and sharing those identifiers and information with its time-keeping vendor, without her consent.

29. Defendant diminished the value of Plaintiff's biometric identifiers and information by storing them without publishing data retention and destruction policies required by the Biometric Information Privacy Act.

30. Based on Defendant's violations of the informed-consent and data destruction/retention publishing policies of the Biometric Information Privacy Act, Plaintiff experiences emotional distress over whether Defendant is currently storing, disposed of, or will eventually dispose of, their biometric identifiers and information securely.

31. Plaintiff also experiences emotional distress because she recognizes that she will not learn of any data breach that compromises her biometric identifiers and information until *after* that data breach has occurred.

CLASS ACTION ALLEGATIONS

32. Plaintiff seeks to represent a class of Defendant's employees in Illinois who scanned their fingerprints in Defendant's biometric time clock system ("the Class").

33. Plaintiff and the Class are similar to one another because they were all subject to the same allegedly illegal practices: being required to scan their fingerprints in Defendant's biometric time clock system despite Defendant failing to adhere to the requirements of the Biometric Information Privacy Act.

34. The Class includes more than 75 members.

35. As a result, the Class is so numerous that joining of all class members in one lawsuit is not practical.

36. The issues involved in this lawsuit present common questions of law and fact, including: whether Defendant required the Class to use their fingerprints to clock in and out during shifts; whether Defendant collected the Class's "biometric identifiers" or "biometric information" under the Biometric Information Privacy Act; and whether Defendant complied with the procedures in 740 ILCS 14/15(a), (b), and (d) of the Biometric Information Privacy Act.

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

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

39. If individual actions were required to be brought by each member of 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.

40. Accordingly, a class action is an appropriate method for the fair and efficient adjudication of this lawsuit and distribution of the common fund to which the Class is entitled.

41. The books and records of Defendant are material to Plaintiff's case as they disclose how and when Plaintiff and the Class scanned their fingerprints 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.

42. Plaintiff and her counsel will fairly and adequately protect the interests of the Class.

43. Plaintiff retained counsel experienced in complex class action litigation.

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

44. Plaintiff realleges and incorporates the previous allegations of this Complaint.

45. Defendant is a "private entity" under the Biometric Information Privacy Act. 740 ILCS 14/10.

46. Plaintiff's and the Class's fingerprints qualify as "biometric identifier[s]" as defined by the Biometric Information Privacy Act. 740 ILCS 14/10.

47. Defendant has "biometric information" from Plaintiff and the Class through its acquisition and retention of information based on Plaintiff's and the Class's fingerprints.

48. Defendant violated the Biometric Information Privacy Act by capturing or collecting Plaintiff's and the Class's fingerprints and information based on their fingerprints without first informing them in writing that Defendant was doing so.

49. Defendant violated the Biometric Information Privacy Act by capturing or collecting Plaintiff's and the Class's fingerprints and information based on their fingerprints without first informing them in writing of the purpose of Defendant doing so and the length of time Defendant would store and use Plaintiff's and the Class's biometric identifiers and/or biometric information.

50. Defendant violated the Biometric Information Privacy Act by capturing or collecting Plaintiff's and the Class's fingerprints and information based on their fingerprints without first obtaining their written consent or other release authorizing Defendant to capture or collect Plaintiff's and the Class's biometric identifiers and/or biometric information.

51. Defendant knew or should have known of the requirements of the Biometric Information Privacy Act.

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

A. Awarding liquidated monetary damages to Plaintiff and the Class for each violation of the Biometric Information Privacy Act as provided by 740 ILCS 14/20(1)-(2);

B. Enjoining Defendant from committing further violations of the Biometric Information Privacy Act 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)

52. Plaintiff realleges and incorporates the previous allegations of this Complaint.

53. Defendant is a "private entity" under the Biometric Information Privacy Act. 740 ILCS 14/10.

54. Plaintiff's and the Class's fingerprints qualify as "biometric identifier[s]" as defined by the Biometric Information Privacy Act. 740 ILCS 14/10.

55. Defendant has "biometric information" from Plaintiff and the Class through its acquisition and retention of information based on Plaintiff's and the Class's fingerprints.

56. Defendant violated the Biometric Information Privacy Act by possessing Plaintiff's and the Class's fingerprints and information based on their fingerprints without creating a written policy, made available to the public, establishing a retention schedule and destruction guidelines for its possession of biometric identifiers and information.

57. Defendant knew or should have known of the requirements of the Biometric Information Privacy Act.

58. As a result, Defendant's violations of the Biometric Information Privacy Act were

reckless or, in the alternative, negligent.

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

A. Awarding liquidated monetary damages to Plaintiff and the Class for each violation of the Biometric Information Privacy Act as provided by 740 ILCS 14/20(1)-(2);

B. Enjoining Defendant from committing further violations of the Biometric Information Privacy Act 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)

59. Plaintiff realleges and incorporates the previous allegations of this Complaint.

60. Defendant is a "private entity" under the Biometric Information Privacy Act. 740 ILCS 14/10.

61. Plaintiff's and the Class's fingerprints qualify as "biometric identifier[s]" as defined by the Biometric Information Privacy Act. 740 ILCS 14/10.

62. Defendant has "biometric information" from Plaintiff and the Class through its acquisition and retention of information based on Plaintiff's and the Class's fingerprints.

63. Defendant violated the Biometric Information Privacy Act by disclosing or otherwise disseminating Plaintiff's and the Class's fingerprints and information based on their fingerprints to Defendant's time-keeping vendor without first obtaining their consent for that disclosure or dissemination.

64. Defendant knew or should have known of the requirements of the Biometric Information Privacy Act.

65. As a result, Defendant's violations of the Biometric Information Privacy Act were reckless or, in the alternative, negligent.

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

A. Awarding liquidated monetary damages to Plaintiff and the Class for each violation of the Biometric Information Privacy Act as provided by 740 ILCS 14/20(1)-(2);

B. Enjoining Defendant from committing further violations of the Biometric Information Privacy Act 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: August 6, 2019

/s/ Douglas M. Werman
One of Plaintiff's Attorney

Douglas M. Werman (dwerman@flsalaw.com)
Maureen A. Salas (msalas@flsalaw.com)
Zachary C. Flowerree (zflowerree@flsalaw.com)
Sarah J. Arendt (sarendt@flsalaw.com)
WERMAN SALAS P.C.
77 West Washington, Suite 1402
Chicago, Illinois 60602
(312) 419-1008

Attorneys for Plaintiff