YES / (NO)

EXHIBITS

CASE NO. 2020 CH 2768

DATE: 3/6/20

CASE TYPE: CLASS ACTION

PAGE COUNT: 15

CASE NOTE

ALDI

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

8760019

MICHELLE SEDORY individually and on behalf of all others similarly situated,

Plaintiff ,

v.

ALDI INC.

Defendant ,

Case No.: 2020CH02768

CLASS ACTION COMPLAINT

Plaintiff Michelle Sedory ("Michelle", "Plaintiff") brings this Class Action Complaint against Aldi Inc., ("Aldi") to put a stop to its unlawful collection, use, and storage of Plaintiff's and the putative Class members' sensitive biometric data. Plaintiff alleges as follows upon personal knowledge as to Plaintiff's own acts and experiences and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. Defendant Aldi is a discount grocery store. It employs nearly 25,000 individuals and it has over 1,000 facilities located in the United States.

2. When employees work at certain locations for Aldi, they are required to scan their fingerprint in its biometric time tracking system as a means of authentication, instead of using only key fobs or other identification cards.

3. While there are tremendous benefits to using biometric time clocks in the workplace, there are also serious risks. Unlike key fobs or identification cards—which can be

changed or replaced if stolen or compromised—fingerprints are unique, permanent biometric identifiers associated with the employee. This exposes employees to serious and irreversible privacy risks. For example, if a fingerprint database is hacked, breached, or otherwise exposed, employees have no means by which to prevent identity theft and unauthorized tracking. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches or misuses – employees have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

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

5. A black market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-ofidentity-theft/?utm_term=.b3c70259f138.

6. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than $8 and in as little as 10 minutes. Rachna Khaira,

Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details, The Tribune (Jan. 4, 2018), *available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-accessto-billion-aadhaar-details/523361.html.

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

8. Despite this law, Aldi disregards its employees' statutorily protected privacy rights and unlawfully collects, stores, and uses their biometric data in violation of the BIPA. Specifically, Aldi has violated (and continues to violate) the BIPA because it did not:

- Properly inform Plaintiff and the Class members in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, and used, as required by the BIPA;
- Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff and the Class's fingerprints, as required by the BIPA; nor
- Receive a written release from Plaintiff or the members of the Class to collect, capture, or otherwise obtain fingerprints, as required by the BIPA.

9. Accordingly, this Complaint seeks an order: (i) declaring that Defendant's conduct violates the BIPA; (ii) requiring Defendant to cease the unlawful activities discussed herein; and (iii) awarding liquidated damages to Plaintiff and the proposed Class.

PARTIES

10. Plaintiff is a natural person residing in the state of the State of Illinois.

11. Defendant Aldi operates in Illinois.

JURISDICTION AND VENUE

12. This Court has jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 because Defendant conducts business transactions in Illinois, and has committed tortious acts in Illinois.

13. Venue is proper because Defendant operates throughout Illinois.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

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

15. In late 2007, a biometrics company called Pay By Touch—which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records—which, are unique biometric identifiers, can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who had used that company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that unique biometric identifiers could now be sold to unknown third parties.

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

17. The BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it *first*:

> (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information.

740 ILCS 14/15(b).

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

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

20. The BIPA also establishes standards for how employers must handle Illinois employees' biometric identifiers and biometric information. *See* 740 ILCS 14/15(c)–(d). For instance, the BIPA requires companies to develop and comply with a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting

such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

21. Ultimately, the BIPA is simply an informed consent statute. Its narrowly tailored provisions place no absolute bar on the collection, sending, transmitting or communicating of biometric data. For example, the BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does the BIPA limit to whom biometric data may be collected, sent, transmitted, or stored. The BIPA simply mandates that entities wishing to engage in that conduct must make proper disclosures and implement certain reasonable safeguards.

II. Aldi Violates the Biometric Information Privacy Act.

22. By the time the BIPA passed through the Illinois Legislature in mid-2008, many companies who had experimented with using biometric data as an authentication method stopped doing so, at least for a time. That is because Pay By Touch's bankruptcy, described in Section I above, was widely publicized and brought attention to consumers' discomfort with the use of their biometric data.

23. Unfortunately, Aldi specifically failed to take note of the passage of the BIPA. Aldi continues to collect, store, and use its employees' biometric data in violation of the BIPA.

24. Specifically, when employees work at certain Aldi locations, they are required to have their fingerprints scanned in order to enroll them in its fingerprint database.

25. Aldi uses an employee time tracking system that requires employees to use their fingerprints as a means of authentication. Unlike a traditional time clock, employees have to use their fingerprint to "punch" in to or out of work.

26. Aldi failed to inform its employees of the complete purposes for which it collects their sensitive biometric data or to whom the data is disclosed, if at all.

27. Aldi similarly failed to provide its employees with a written, publicly available policy identifying its retention schedule, and guidelines for permanently destroying its employees' fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by the BIPA. An employee who leaves the company does so without any knowledge of when their biometric identifiers will be removed from Aldi databases—or if they ever will be.

28. The Pay By Touch bankruptcy that catalyzed the passage of the BIPA highlights why conduct such as Aldi —whose employees are aware that they are providing biometric identifiers but are not aware of to whom or the full extent of the reasons they are doing so—is so dangerous. That bankruptcy spurred Illinois citizens and legislators to realize a critical point: it is crucial for people to understand when providing biometric data who exactly is collecting it, who it will be transmitted to, for what purposes, and for how long. But Aldi disregards these obligations, and instead unlawfully collects, stores, and uses its employees' biometric identifiers and information without proper consent.

29. Ultimately, Aldi disregards its employees' statutorily protected privacy rights by violating the BIPA.

FACTS SPECIFIC TO PLAINTIFF

30. Plaintiff worked for Aldi, in Illinois.

31. As an employee, Aldi required Plaintiff to scan Plaintiff's fingerprint so that it could use it as an authentication method to track time. Aldi subsequently stored Plaintiff's fingerprint data in its databases.

32. Each time Plaintiff began and ended a workday, Aldi required a scan of Plaintiff's fingerprints.

33. Aldi never informed Plaintiff of the specific limited purposes or length of time for which it collected, stored, or used fingerprints.

34. Similarly, Aldi never informed Plaintiff of any biometric data retention policy it developed, nor whether it will ever permanently delete fingerprints.

35. Plaintiff never signed a written release allowing Aldi to collect or store fingerprints.

36. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Aldi violations of the BIPA alleged herein.

37. Plaintiff now seeks liquidated damages under BIPA as compensation for the injuries Aldi has caused.

CLASS ALLEGATIONS

38. **Class Definition**: Plaintiff brings this action pursuant to 735 ILCS 5/2-801 on behalf of themselves and a Class of similarly situated individuals, defined as follows:

> All residents of the State of Illinois who had their fingerprints collected, captured, received, otherwise obtained, or disclosed by Aldi while residing in Illinois.

The following people are excluded from the Class: (1) any Judge presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

39. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but it is clear that individual joinder is impracticable. Defendant has collected, captured, received, or otherwise obtained biometric identifiers or biometric information from at least

hundreds of employees who fall into the definition of the Class. Ultimately, the Class members will be easily identified through Defendant's records.

40. **Commonality and Predominance**: 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 of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a) whether Defendant collected, captured, or otherwise obtained Plaintiff's and the Class' biometric identifiers or biometric information;

b) whether Defendant properly informed Plaintiff and the Class of its purposes for collecting, using, and storing their biometric identifiers or biometric information;

c) whether Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiff's and the Class' biometric identifiers or biometric information;

d) whether Defendant has sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometric identifiers or biometric information;

e) 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 their last interaction, whichever occurs first;

f) whether Defendant complies with any such written policy (if one exists); and

g) whether Defendant used Plaintiff's and the Class' fingerprints to identify them.

41. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class and have retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to

vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of the other members of the Class.

42. **Appropriateness**: This class action is appropriate for certification because class proceedings are superior to all others available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in their Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

FIRST CAUSE OF ACTION Violation of BIPA Section 15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

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

44. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the

company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

45. Defendant fails to comply with these BIPA mandates.

46. Defendant is an entity registered to do business in Illinois and thus qualifies as a "private entity" Under BIPA. *See* 740 ILCS 14/10.

47. Plaintiff is an individual who had her "biometric identifiers" (in the form of their fingerprints) collected by Defendant, as explained in detail above, *supra*. *See* 740 ILCS 14/10.

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

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

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

51. On behalf of themselves and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740

ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION

Violation of BIPA Section 15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

52. Plaintiff incorporate the foregoing allegations as if fully set forth herein.

53. BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject...in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject...in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information..." 740 ILCS 14/15(b) (emphasis added).

54. Defendant fails to comply with these BIPA mandates.

55. Defendant is an entity registered to do business in Illinois and thus qualifies as a "private entity" Under BIPA. *See* 740 ILCS 14/10.

56. Plaintiff is an individual who had "biometric identifiers" (in the form of fingerprints) collected by Defendants, as explained in detail in Sections II and III, *supra*. *See* 740 ILCS 14/10.

57. Plaintiff's biometric identifiers were used to identify them and, therefore, constitute

"biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

58. Defendant systematically and automatically collected, used, stored, and disclosed Plaintiff's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

59. Defendant did not inform Plaintiff in writing that their biometric identifiers and/or biometric information were being collected, stored, used, and disseminated, nor did Defendant inform Plaintiff in writing of the specific purpose and length of term for which biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

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

61. On behalf of themselves and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring each Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff individually and for the Class, respectfully request that the Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing Plaintiff's counsel as Class Counsel;

B. Declaring that Defendant's actions, as set out above, violate the BIPA;

C. Awarding damages for each of Defendant's violations of the BIPA, pursuant to 740 ILCS 14/20;

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

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

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

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

Dated: March 2, 2020

Respectfully submitted,

MICHELLE SEDORY, individually and on behalf of all others similarly situated,

By: /s/ David Fish
One of Plaintiff's Attorneys

David Fish
dfish@fishlawfirm.com
John Kunze
kunze@fishlawfirm.com

Mara Baltabols
mara@fishlawfirm.com
THE FISH LAW FIRM, P.C.
200 East Fifth Avenue, Suite 123
Naperville, Illinois 60563
Tel: 630.355.7590
Fax: 630.778.0400
admin@fishlawfirm.com