

Return Date: No return date scheduled
Hearing Date: 7/8/2021 9:30 AM - 9:30 AM
Courtroom Number: 2408
Location: District 1 Court
Cook County, IL

12-Person Jury

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

FILED
3/10/2021 3:16 PM
IRIS Y. MARTINEZ
CIRCUIT CLERK
COOK COUNTY, IL
2021CH01145

RONESHA SMITH, on behalf of herself and
all others similarly situated,

Plaintiff,

v.

SIGNATURE SYSTEMS, INC.

Defendant.

Case No.: 2021CH01145

12526550

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Ronesha Smith, individually and on behalf of all others similarly situated, brings this Class Action Complaint for violations of the Illinois Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1 *et seq.*, against Signature Systems, Inc. (“Defendant”), and alleges as follows based on personal knowledge as to herself, on the investigation of her counsel and the advice and consultation of certain third-party agents as to technical matters, and demands trial by jury:

NATURE OF ACTION

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in collecting, storing and using Plaintiff’s and other similarly situated individuals’ biometric identifiers¹ and biometric information² (referred to collectively at times as “biometrics”) without obtaining the requisite prior informed written consent or providing the requisite data retention and destruction policies, in direct violation of BIPA.

2. The Illinois Legislature has found that “[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information.” 740 ILCS 14/5(c).

¹ A “biometric identifier” is a personal feature unique to an individual, such as a fingerprint, handprint, iris scan, scan of face geometry, among others.

² “Biometric information” is any information captured, converted, stored or shared based on a person’s biometric identifier used to identify an individual.

FILED DATE: 3/10/2021 3:16 PM 2021CH01145

“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.” *Id.*

3. In recognition of these concerns over the security of individuals’ biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Defendant may not obtain and/or possess an individual’s biometrics unless it: (1) informs that person in writing that biometric identifiers or information will be collected or stored, *see id.*; (2) informs that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, stored and used, *see id.*; (3) receives a written release from the person for the collection of his or her biometric identifiers or information, *see id.*; and (4) publishes publicly available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information, *see* 740 ILCS 14/15(a). Further, the entity must store, transmit and protect an individual’s biometric identifiers and biometric information using the same standard of care in the industry and in a manner at least as protective as the means used to protect other confidential and sensitive information. *Id.* 14/15(e). Finally, the entity is expressly prohibited from selling, leasing, trading or otherwise profiting from the individual’s biometrics. *Id.* 15/15(c).

4. In direct violation of each of the foregoing provisions of § 15(a) and § 15(b) of BIPA, Defendant is actively collecting, storing, and using – without providing notice, obtaining informed written consent or publishing data retention policies – the fingerprint and associated personally identifying information of thousands of Illinois residents employed by Defendant’s clients. Initially collected from employees prior to or early on in their employment, employees’ fingerprint are stored by Defendant in an electronic database and used to, *inter alia*, allow Defendant’s clients’ employees to clock in and clock out of work. Specifically, to allow its client’s employees to clock in and clock out of work in Illinois and/or access point-of-sale systems, Defendant collects (via an electronic scanning device) the employee’s fingerprint and stores the

fingerprint in its fingerprint database along with credentials corresponding to that employee. Then, when an employee places his or her fingerprint on one of Defendant's scanning devices to clock in and clock out of work and/or access a point-of-sale system, he or she is only granted access if the collected fingerprint matches a fingerprint stored in Defendant's database (which was collected during enrollment).

5. If Defendant's database of digitized fingerprints were to fall into the wrong hands, by data breach or otherwise, individuals to whom these sensitive biometric identifiers belong could have their identities stolen or their financial and other highly personal information breached and used for nefarious purposes. BIPA confers on Plaintiff and all other similarly situated Illinois residents a right to know of such risks, which are inherently presented by the collection and storage of biometrics, and a right to know how long such risks will persist after their employment with the company ends. Yet Defendant never adequately informed any of the Illinois residents whose biometrics it collected and stored of Defendant's biometrics collection practices, never obtained written consent from any of these individuals regarding its biometric practices, and never provided any data retention or destruction policies to any of these individuals.

6. Plaintiff brings this action to prevent Defendant from further violating the rights of Illinois residents, and to recover statutory damages for Defendant's unauthorized collection, storage and use of these individuals' biometrics in violation of BIPA.

PARTIES

7. Plaintiff is, and has been at all relevant times, a resident and citizen of Chicago, Illinois.

8. Defendant is a corporation that maintains its headquarters in Warminster, Pennsylvania. Defendant is the owner, operator, and vendor of point-of-sale systems for commercial enterprises including restaurants, casinos, and other hospitality venues.

JURISDICTION AND VENUE

9. The Court has personal jurisdiction over Defendant because the fingerprints that give rise to this lawsuit were and still are (1) collected by Defendant at a facility in Cook County,

Illinois, (2) stored by Defendant at a facility in Cook County, Illinois, and (3) used by Defendant at facilities in Cook County, Illinois.

10. The Chancery Division is the appropriate venue for this action because it is a class action and, additionally, because it seeks declaratory and injunctive relief.

FACTUAL BACKGROUND

I. Illinois's Biometric Information Privacy Act

11. In 2008, Illinois enacted BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA makes it unlawful for a company to, *inter alia*, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers 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 or the subject's legally authorized representative."

740 ILCS 14/15 (b).

12. Section 15(a) of BIPA also provides:

A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

13. As alleged below, Defendant's practices of collecting, storing and using individuals' biometric identifiers (specifically, fingerprints) and associated biometric information without informed written consent violate all three prongs of § 15(b) of BIPA. Defendant's failure

to provide a publicly available written policy regarding their schedule and guidelines for the retention and permanent destruction of individuals' biometric identifiers and biometric information also violates § 15(a) of BIPA.

II. Defendant Violates Illinois's Biometric Information Privacy Act

14. Unbeknownst to the average consumer, and in direct violation of § 15(b)(1) of BIPA, Defendant scans and collects, and then indefinitely stores in an electronic database, digital copies of its client's employees' fingerprints during the initial process of enrolling these individuals in its databases of fingerprints in Illinois, as well as whenever employees clock in and clock out of work and/or attempt to access a point-of-sale system at one of Defendant's clients' Illinois-based locations where Defendant's biometrics technology is used – all without ever informing anyone of this practice in writing.

15. In direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, Defendant never informed Illinois residents who had their fingerprints collected of the specific purpose and length of term for which their biometric identifiers or information would be collected, stored and used, nor did Defendant obtain a written release from any of these individuals.

16. In direct violation of § 15(a) of BIPA, Defendant does not have written, publicly available policies identifying their retention schedules, or guidelines for permanently destroying any of these biometric identifiers or biometric information.

III. Plaintiff Ronesha Smith's Experience

17. Jimmy John's, Inc. ("Jimmy John") is a nation-wide fast-food franchisor. Jimmy John's mandates the use of Defendant's point-of-sale system as a franchise requirement.

18. From approximately July 2019 through September 2019, Plaintiff was employed by a Jimmy John's franchised restaurant in Evergreen Park, Illinois (the "Evergreen Park Facility").

19. During the course of Plaintiff's employment at the Evergreen Park Facility, Defendant, through its point-of-sale system, scanned and collected, and stored in an electronic database, digital copies of Plaintiff's fingerprints.

20. Plaintiff used her fingerprint to clock in and clock out of work at the Evergreen Park Facility on a daily basis during her employment. Plaintiff was required to place her finger on a fingerprint scanner, which scanned, collected and stored her fingerprint each time she attempted to clock in and clock out of work at the Evergreen Park Facility. Defendant's sophisticated fingerprint matching technology then compared Plaintiff's scanned fingerprint against the fingerprints previously stored in Defendant's fingerprint database, at which point Plaintiff was able to clock in and clock out of work at Defendant's Evergreen Park Facility.

21. Plaintiff never consented, agreed or gave permission – written or otherwise – to Defendant for the collection or storage of her unique biometric identifiers or biometric information.

22. Further, Defendant never provided Plaintiff with nor did she ever sign a written release allowing Defendant to collect or store her unique biometric identifiers or biometric information.

23. Likewise, Defendant never provided Plaintiff with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of her unique biometric identifiers or biometric information.

24. By collecting Plaintiff's unique biometric identifiers or biometric information without her consent, written or otherwise, Defendant invaded Plaintiff's statutorily protected right to maintain control over her biometrics.

25. Finally, Defendant never provided plaintiff with a retention schedule and/or guidelines for permanently destroying her biometric identifiers and biometric information.

CLASS ALLEGATIONS

26. **Class Definition:** Plaintiff brings this action pursuant to 735 ILCS 5/2-801 on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

All individuals who had their fingerprints collected, captured, received, or otherwise obtained, and/or stored, by Defendant in Illinois.

The following are excluded from the Class: (1) any Judge presiding over this action and members of his or her family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parent has a controlling interest (as well as current or former employees, 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.

27. **Numerosity:** Pursuant to 735 ILCS 5/2-801(1), the number of persons within the Class is substantial, believed to amount to at least hundreds and possibly thousands of persons. It is, therefore, impractical to join each member of the Class as a named Plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

28. **Commonality and Predominance:** Pursuant to 735 ILCS 5/2-801(2), there are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any class member include, but are not limited to, the following:

- (a) whether Defendant collected or otherwise obtained Plaintiff's and the Class's fingerprints;
- (b) whether Defendant collected or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;
- (c) whether Defendant properly informed Plaintiff and the Class that it collected, used, and stored their biometric identifiers or biometric information;

- (d) whether Defendant obtained a written release (as defined in 740 ILCS 1410) to collect, use, and store 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 3 years of their last interaction, whichever occurs first;
- (f) whether Plaintiff's and the Class's biometric information that Defendant collected was capable of identifying them; and
- (g) whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

29. **Adequate Representation:** Pursuant to 735 ILCS 5/2-801(3), Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiff and her counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff is able to fairly and adequately represent and protect the interests of such a Class. Neither Plaintiff nor her counsel has any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Class or additional claims as may be appropriate.

30. **Superiority:** Pursuant to 735 ILCS 5/2-801(4), a class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed.

Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with BIPA.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/1, *et seq.*
(On Behalf of Plaintiff and the Class)

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

32. BIPA makes it unlawful for any private entity 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).

33. Defendant is a corporation and thus qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

34. Plaintiff and the Class members are individuals who had their fingerprints, i.e., “biometric identifiers,” collected and stored by Defendant. *See* 740 ILCS 14/10.

35. Plaintiff and the Class members are individuals who had their “biometric information” collected and stored by Defendant in the form of digitally encrypted code, derived from Plaintiff’s and the Class members’ fingerprints, that uniquely identifies the individual to whom a particular fingerprint belongs.

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

37. In fact, Defendant failed to properly inform Plaintiff or the Class in writing that their biometric identifiers and/or biometric information were being collected, stored, or otherwise obtained, nor did Defendant inform Plaintiff or the 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, as required by 740 ILCS 14/15(b)(1)-(2).

38. In addition, Defendant does not publicly provide a retention schedule or guidelines for permanently destroying the biometric identifiers and/or biometric information of Plaintiff or the Class members, as required by BIPA. *See* 740 ILCS 14/15(a). The failure by Defendant to provide Plaintiff and the Class members with a retention schedule or guidelines for permanently destroying Plaintiff's or the Class members' biometric identifiers or biometric information constitutes an independent violation of the statute.

39. Each instance in which Defendant collected, stored, used, or otherwise obtained Plaintiff's and/or the Class's biometric identifiers and biometric information as described herein constitutes a separate violation of the statute and of the right of Plaintiff and each Class member to maintain control over these biometric identifiers and biometric information, as set forth in BIPA, 740 ILCS 14/1, *et seq.*

40. On behalf of herself and the proposed Class members, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements, including BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein, and for the provision of the requisite written disclosure to consumers; (2) statutory damages of \$1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) (or, alternatively, of \$5,000.00 for each and every violation of BIPA to the extent committed

intentionally or recklessly pursuant to 740 ILCS 14/20(2)); and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Ronesha Smith, on behalf of herself and the proposed Class, respectfully requests that this 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 her counsel as Class Counsel;

B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;

C. Awarding statutory damages of \$1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) (or, alternatively, of \$5,000.00 for each and every violation of BIPA to the extent committed intentionally or recklessly pursuant to 740 ILCS 14/20(2));

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

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: March 10, 2021

Respectfully submitted,

/s/ Carl V. Malmstrom

**WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLC**
Attorney No. 38819
Carl V. Malmstrom
111 W. Jackson Blvd., Suite 1700

Chicago, IL 60604
Tel: (312) 391-5059
Fax: (212) 686-0114
malmstrom@whafh.com

Local Counsel for Plaintiff and the Putative Class

HEDIN HALL LLP
Frank S. Hedin*
David W. Hall*
Arun G. Ravindran*
1395 Brickell Avenue, Ste 1140
Miami, Florida 33131
Tel: (305) 357-2107
Fax: (305) 200-8801
E-mail: fhedin@hedinhall.com
dhall@hedinhall.com

**Pro Hac Vice Application Forthcoming*

Counsel for Plaintiff and the Putative Class