IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

TYRONE BREWER, on behalf of himself and all others similarly situated,	)	
Plaintiff,	)	
	)	Case No. 21-cv-535
v.	)	
	)	Jury Demanded
PEPPERIDGE FARM, INCORPORATED,	)	
Defendant	)	

CLASS ACTION COMPLAINT

Plaintiff Tyrone Brewer, on behalf of himself and a putative class, brings this Class Action Complaint against Defendant Pepperidge Farm, Incorporated ("Pepperidge Farm") for its violations of the Illinois Biometric Privacy Act, and alleges the following:

NATURE OF THE ACTION

1. When employees are hired at Pepperidge Farm they have their fingerprints scanned into one of its biometric time clocks.

2. Each day the employees press their finger into the time clock to "punch" in and out and to get through a door, so that Pepperidge Farm may record its employees' arrival, departure, and break times.

3. While the use of fingerprint scans may be more secure for the building than key fobs, identification cards, or combination codes, the use of biometric identifiers in the workplace entails risks for the employees. Fingerprints are permanent, unique biometric identifiers that will be associated with the employee forever, whereas other security measures that may be misplaced

or stolen can be deactivated. Keeping employees' biometric identifiers on file exposes them to serious privacy risks like identity theft and unauthorized tracking.

4. Illinois enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA") to regulate private entities that collect and store biometric identifiers, such as fingerprints.

5. Pepperidge Farm violated their employees' privacy rights by unlawfully collecting, storing, and/or using their biometric data and information not in accordance with BIPA.

PARTIES

6. Plaintiff Tyrone Brewer is a natural person and resident of this district, and former employee of the defendant.

7. Defendant Pepperidge Farm, Incorporated is a Connecticut corporation, with its headquarters in Connecticut, manufacturing plants in Illinois and Pennsylvania, and its registered agent C T Corporation System located at 208 S LaSalle Street, Suite 814, Chicago, Illinoi 60604.

JURISDICTION AND VENUE

8. This Court has diversity jurisdiction under 28 U.S.C. § 1332(a) over the Defendant.

9. The parties are all completely diverse: Tyrone Brewer is a citizen of Illinois. Pepperidge Farm is a Connecticut corporation with its principal place of business also in Connecticut.

10. An individual may recover between $1,000 and $5,000 in statutory damages for *each* violation of BIPA. Mr. Brewer estimates he scanned his hand 6 times a day, 6 days a week, for his three-week term of employment. Based on the length of time Mr. Brewer worked for Defendant and the number of times his handprint was scanned each day, the statutory damages he is entitled to far exceed $75,000.

11. This Court has personal jurisdiction over Defendant because it conducts a substantial amount of business here which forms the basis of Plaintiff's claims. Defendant's Illinois manufacturing plant is located at 230 2nd St, Downers Grove, IL 60515.

12. Venue is proper here under 28 U.S.C. § 1391(b)(2) because a substantial amount of the acts and omissions giving rise to the claims occurred in Illinois.

PLAINTIFF'S FACTUAL ALLEGATIONS

13. Plaintiff was employed at Pepperidge Farm for May of 2020, contracted by a temporary agency located in the same building.

14. At the start of his employment, his handprint was scanned and saved by the biometric time clock system. His handprint was then used to identify him during his workhours, when he needed to get through the building door.

15. Each time Plaintiff needed to access the building, Plaintiff had to scan his hand on a biometric time clock that looked like a 3-foot-tall podium and enter in a six-digit code, which was the last six digits of his social security number, to open the door.

16. Defendant was in actual possession of Plaintiff's biometric information contained in the biometric time clock system.

17. Plaintiff saw his coworkers use the same scanner as he did and estimates that he and the other class members were asked to scan their hands three to six times per day over the course of their employment.

18. More than ten years ago, the Illinois Legislature recognized the promises and perils of biometric identification technology. It passed the Biometric Information Privacy Act, 740 ILCS § 14/1 *et seq.*, to establish and safeguard Illinois' residents absolute right to control their biometric data.

19. Under the act, a fingerprint or a handprint are biometric identifier. *Id.* at § 14/10.

20. Biometric information is any information derived from a biometric identifier, regardless of how it is captured, stored, or shared. *Id.*

21. Defendant used the scanner system to capture the handprints of its numerous employees and store them for future use.

22. Plaintiff's and Class members' handprints were obtained by Defendant and stored on Defendant's equipment to later identify each individual.

23. Each time Plaintiff scanned his handprints using the scanner, the Defendant obtained his handprint.

24. Under the act, a private entity in possession of either biometric identifiers or information must develop a written policy, available to the public, establishing a retention schedule and guidelines for permanently destroying the information or identifiers. *Id.* § 14/15(a). Private entities must also comply with that policy.

25. Defendant has not provided any policy establishing either a retention schedule or guidelines for permanently destroying the biometric data. Plaintiff was not informed of any such policy and no policy was made publicly available. Based on these facts, Defendant did not develop any policy regarding biometric information, nor could they have complied with any policy.

26. Under the act, a private entity is prohibited from collecting, capturing, or otherwise obtaining a person's biometric information or identifier unless it first: a) informs the subject in writing that the information or identifier is being collected or stored; b) informs the subject in writing of the specific purpose and length of term for which the information or identifier is being

collected, stored, or used; and, c) receives a written release from the subject of the information or identifier. *Id.* at § 14/15(b).

27. Plaintiff or any member of the Class were not, at any relevant time, informed in writing of any of the information required under § 14/15(b). Neither the Plaintiff nor members of the putative Class executed a written release to their employer.

28. Under the act, a private entity in possession of biometric information or identifiers may not disclose, redisclose, or disseminate a person's biometric identifier or information unless the person consents to the disclosure or re-disclosure. *Id.* at § 14/15(d).

29. Specifically, on information and belief, Defendant allowed other employees and third-parties (for example, the on-site staffing company that hired Plaintiff) access to the print and scan database and disseminated the biometric information by transmitting it both internally and externally.

30. Plaintiff Brewer and the putative class members never consented to these disclosures.

31. Lastly, a private entity in possession of biometric identifiers or information must store, transmit, and protect from disclosure all biometric identifiers and information using a reasonable standard of care and in the same way the private entity stores, transmits, and protects other sensitive information. *Id.* at § 14/15(e).

32. On information and belief, access to the fingerprint database was essentially open to large numbers of the Defendant's employees, agents, and subcontractors. Defendant did not store, transmit, or protect the handprint database in the same way it would do so to other sensitive information. For example, Defendant did not encrypt the biometric data they stored on their servers.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.