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

FAITH MENDENHALL, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No.** 2024CH00998
v.	)	
XENIAL, INC. and GLOBAL PAYMENTS INC.	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff Faith Mendenhall ("Plaintiff" or "Mendenhall") individually and on behalf of all others similarly situated (the "Class"), by and through her attorneys, brings the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against Xenial, Inc. ("Xenial") and Global Payments Inc. ("Global Payments") (together with Xenial, "Defendants"), their subsidiaries and affiliates, to redress and curtail Defendants' unlawful collection, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric identifiers and biometric information (collectively referred to herein as "biometric data"). Plaintiff alleges as follows upon personal knowledge as to herself and her own acts and experiences, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. BIPA addresses the dangers posed by the mishandling of biometric data[1] by

[1] Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and 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. *Id.* For ease of reference, "biometric data" and "biometrics" as used herein shall refer to both biometric identifiers and information.

providing a right of action to any person who is subjected to a violation of the Act within the State of Illinois. 740 ILCS § 14/20.

2. As relevant here, private entities that collect, obtain, store, or otherwise possess an individual's biometric data violate BIPA when they (i) fail to develop, publicly disclose, and comply with "a retention schedule and guidelines for permanently destroying biometric identifiers and information" (740 ILCS § 14/15(a)); (ii) obtain biometric data without first providing adequate written notice and obtaining a written release (740 ILCS §§ 14/15(b), 14/10); and (iii) share biometric data without first obtaining the individual's informed consent (740 ILCS § 14/15(d)).

3. This action seeks to remedy Defendants' illegal practice of disregarding Plaintiff's and all other similarly situated individuals' statutorily protected privacy rights in violation of each of these sections.

4. Defendant Xenial is a technology platform that offers restaurant and food-management hardware, software and services to customers in the quick service and fast casual food service management industry.

5. Defendant Global Payments is a Fortune 500 Company and vendor of hardware, software, and service solutions intended to power businesses across a wide swath of sectors, including retail, restaurant, healthcare, financial services, and education, among others. Global Payments is Xenial's corporate parent.

6. The Xenial platform provides a complete restaurant management software solution that includes front-of-house biometric-enabled Point-of-Sale ("POS") systems, which are comprised of POS terminals with fingerprint readers and cloud-based POS software.[2] Xenial

[2] *See Serve up more business for your restaurant*, GLOBAL PAYMENTS, https://www.globalpayments.com/industries/restaurant (last visited Feb. 16, 2024). In 2018, Global Payments acquired SICOM Systems, Inc., which added "middle-of-house and back-of-house software and other technology capabilities to Xenial's front-of-house platform." *Powering our customers: The technology story behind Global*

also provides back-of-house reporting, inventory management, and staffing and scheduling tools, among other services.

7. Defendants market and deliver their Xenial platform as an "all-in-one" solution, configuring its POS products so that they feature various applications capable of performing management functions, including tracking and managing workers' time and attendance.

8. Each Xenial POS terminal model is configured to be used in conjunction with a biometric fingerprint scanner.

9. Xenial POS terminals that use biometric fingerprint scanners require workers to scan their fingerprints at the biometric-enabled Xenial POS system in order to access the terminal, whether to clock-in or clock-out or to input a food order.

10. These biometric devices function by initially scanning workers' fingerprints to enroll them in a database. Each time the worker subsequently provides his or her fingerprint at the biometric device, the device compares the features of the input fingerprint against the stored fingerprint enrolled to verify the worker's identity.

11. When an employer uses a biometric-enabled Xenial POS system, workers' biometric data is managed, maintained, and stored on Defendants' cloud-based hosted environments and servers.

12. Defendants collected and/or otherwise obtained workers' biometric data captured by the biometric-enabled POS terminals optimized with Xenial's POS software..[3]

Payments, GLOBAL PAYMENTS, https://www.globalpayments.com/insights/2019/02/18/powering-customers-with-a-focus-on-delivering-end-to-end-solutions (last visited Feb. 16, 2024).

[3] *See Global Payments Privacy Notice*, GLOBAL PAYMENTS https://www.globalpayments.com/privacy-statement#zero (last visited Feb. 16, 2024) (including voiceprints, fingerprints or facial scans among the categories of "personal information we collect").

13. Despite their collection of biometric data from workers whose employers utilize its hardware and services, Defendants fail to secure informed consent from subjects of collection, authorizing them to collect, store, use, or disclose their biometric data.

14. Unlike key fobs or identification cards—which can be changed or replaced if stolen or compromised—fingerprints are unique, permanent biometric identifiers associated with each individual. This exposes individuals like Plaintiff to serious and irreversible privacy risks. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed, individuals have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

15. Take, for example, the recent Kronos data breach. Kronos, one of the world's leading providers of biometric timekeeping solutions, succumbed to a ransomware attack in December 2021. The resulting "administrative chaos" suffered by thousands of Kronos' corporate clients extended well into 2022..[4] And for the eight million workers whose personal data was exposed, it may be years before the true extent of their vulnerabilities come to pass. The system breached—Kronos Private Cloud—hosted Kronos's "Workforce Central," where employee biometric data collected for timekeeping purposes is stored.

16. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS § 14/1, *et seq.*, specifically to regulate companies that collect, obtain, store, and use Illinois citizens' biometric data.

17. Notwithstanding the clear and unequivocal requirements of the law, Defendants have disregarded Plaintiff's and other similarly-situated individuals' statutorily protected privacy

[4] *See* Becky Sullivan, *Hackers disrupt payroll for thousands of employers – including hospitals*, (Jan. 5, 2022), https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits.

rights and unlawfully collect, store, use, and disclose Plaintiff's and other similarly-situated individuals' biometric data in violation of BIPA. Specifically, Defendants violated and continue to violate BIPA by:

a. failing to develop, publish, and adhere to a publicly available retention schedule with guidelines for permanently destroying biometric data, as required by Section15(a);

b. failing to obtain from Plaintiff and others similarly situated a written release that notifies them, in writing, that their biometric data was being collected, stored, or otherwise obtained, and specifically why and for how long their biometric data would be collected, stored, and used, as required by Section 15(b); and

c. failing to obtain Plaintiff's informed consent before disclosing, redisclosing, or otherwise disseminating their biometrics to third-parties who host that data, as required by of Section 15(d).

18. Accordingly, Plaintiff, on behalf of herself as well as the putative Class, seeks an Order: (1) declaring that Defendants' conduct violates BIPA; (2) requiring Defendants to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

PARTIES

19. Plaintiff Faith Mendenhall is a natural person and a citizen of the State of Illinois.

20. Defendant Xenial, Inc. is a Delaware corporation with its principal place of business in Charlotte, North Carolina, that conducts business in the State of Illinois.

21. Defendant Global Payments Inc. is a Georgia corporation with its principal place of business in Atlanta, Georgia, that conducts business in the State of Illinois.

JURISDICTION AND VENUE

22. This Court has jurisdiction over Defendants pursuant to 735 ILCS § 5/2-209 because they conduct business transactions in Illinois and committed the statutory violations alleged herein throughout the State of Illinois. In particular, Defendants have sold, leased, and/or

licensed biometric-enabled hardware and software through an automatically renewed subscription service and/or a perpetual license with their customers in Illinois, including Plaintiff's employer, TOMS King (Illinois), LLC, which operated exclusively in Illinois.[5] Under Xenial's Terms and Conditions governing the provision of its services, customers grant Xenial and its authorized subcontractors "a worldwide, perpetual (but revocable hereunder) royalty-free license to host, copy, transmit and display the Customer Data," which is defined as "any data, content or materials of any type that you [the customer] upload, submit or otherwise transmit through the System."[6] These contacts constitute minimum contacts with Illinois such that Defendants purposefully directed their activities at a business operating solely in Illinois with Illinois employees.

23. Venue is proper in Cook County because Defendants conduct the business transactions specified above in Cook County, and Defendants committed the statutory violations alleged herein in Cook County, Illinois.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act

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

---

[5] *See* System Terms and Conditions, XENIAL, https://www.xenial.com/legal/service-terms/Xenial-Consolidated-System-Terms/#:~:text=You%20shall%20not%2C%20and%20shall,laws%2C%20rules%22C%20and%20regulations (last visited Feb. 16, 2024).

[6] *See id.* at Sections 3.2 and 3.3.

25. 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, like other 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 used the 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 their unique biometric identifiers could now be sold to unknown third parties.

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

27. BIPA was enacted due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and—most significantly—the unknown ramifications of biometric technology. It does not, however, prohibit the appropriate use of biometric security and screening measures.

28. BIPA establishes a comprehensive baseline for biometric data protection by making it unlawful for a company to, among other things, collect, capture, store, share, or otherwise obtain, possess or disclose an individual's biometric data without:

a. developing, publishing, and adhering to a publicly available retention schedule with guidelines for permanently destroying biometric data;

b. obtaining a written release from each individual that notifies them, in writing, that their biometric data was being collected, stored, or otherwise obtained, and specifically why and for how long their biometric data would be collected, stored, and used; and

c. obtaining an individual's informed consent before disclosing, redisclosing, or otherwise disseminating their biometrics to other private entities.

See 740 ILCS § 14/15(a), (b), and (d).

29. To ensure compliance, BIPA provides that, for each violation, individuals may recover $1,000 or actual damages, whichever is greater, for negligent violations and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS § 14/20.

30. Biometric identifiers include retina and iris scans, voiceprints, face geometry, hand geometry, and 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. *Id.*

31. BIPA protects individuals' right to privacy over their biometrics and the right to know the precise nature for which their biometrics are used, stored, protected, and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, use, and disclose biometrics, and creates a private right of action for lack of statutory compliance.

32. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric identifiers and biometric information secure. Biometric data, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

II. Defendants' Biometric POS Systems

33. Defendants, at all relevant times, implemented biometric POS systems that required workers to have their biometric identifiers (fingerprints) scanned in order to enroll them in the Xenial platform and authenticate them as authorized users of the systems.

34. Defendants' biometric POS systems recognize workers by their fingerprints.

35. Defendants' biometric hardware and software, like other biometric technology, authenticate workers' identities by capturing and utilizing their biometric identifiers and/or information.

36. Specifically, when workers first use a biometric-enabled Xenial POS system, they are required to have their fingerprint scanned in order to enroll them in Defendants' database. Thereafter, Defendants again collect and/or otherwise obtain workers' fingerprint data upon each subsequent scan of the workers' fingerprints to clock-in and clock-out of work or to otherwise access the POS terminal.

37. Defendants developed and market cloud-based software platforms through which they actively manage, maintain, and store customer data collected from their biometric-enabled POS terminals, including biometric data.

38. Defendants' customers grant Xenial and their third-party "authorized subcontractors" "a worldwide, perpetual (but revocable hereunder) royalty-free license to host, copy, transmit and display" workers' biometric data for the purpose of providing their services.

39. Defendants failed and continue to fail to inform workers enrolled in their biometric-enabled Xenial POS systems that they collect, possess, store, use or otherwise obtain their sensitive biometric data and that they disclose their sensitive biometric data to third-party "authorized subcontractors," as required by BIPA.

40. Defendants failed and continue to fail to inform workers enrolled in their biometric-enabled Xenial POS systems of the purposes and duration for which they collect or obtain their biometric data, as required by BIPA.

41. Defendants failed and continue to fail to obtain written releases from workers enrolled in their Xenial biometric-enabled POS systems before collecting or obtaining their biometric data, as required by BIPA.

42. Defendants did not create or maintain a written, publicly available policy identifying their retention schedule and guidelines for permanently destroying workers' biometric data and did not and will not destroy their biometric data when the initial purpose for collecting or obtaining such data had been satisfied or within three years of the worker's last interaction with the company, as required by BIPA.

43. The Pay by Touch bankruptcy that catalyzed the passage of BIPA, as well as recent data breaches, highlight why such conduct—where individuals are aware that they are providing a fingerprint, but not aware of to whom or for what purposes they are doing so—is dangerous. This bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers, such as their fingerprints, who exactly is collecting their biometric data, where it will be transmitted, for what purposes, and for how long. Defendants disregard these obligations and the statutory rights of workers and instead unlawfully collect, store, use and disclose their biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

44. These violations raise a material risk that Plaintiff and other similarly-situated workers' biometric data will be unlawfully accessed by third parties.

45. By and through the actions detailed above, Defendants disregard Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

III. Plaintiff Faith Mendenhall's Experience

46. Plaintiff Faith Mendenhall worked for TOMS King (Illinois), LLC ("TOMS King") as an hourly-paid staff member from March 2019 to June 2019 at its Burger King franchise location located at 159 US Highway 45 Grayslake, Illinois 60030.

47. Plaintiff was required to scan her fingerprint at a biometric-enabled Xenial POS system to be used as an authentication method to track her time worked and to access the POS terminal at TOMS King's Burger King franchise location in Grayslake, Illinois.

48. Specifically, upon hire, Plaintiff was required to scan and enroll her fingerprint using Xenial's biometric-enabled POS system. Defendants collected and/or otherwise obtained Plaintiff's biometric data upon Plaintiff's enrollment in Xenial's biometric-enabled POS system.

49. Plaintiff was subsequently required to scan her fingerprint at Xenial's biometric-enabled POS system each time she accessed the POS terminal, including to clock in and out of work.

50. Defendants collected and stored Plaintiff's biometric data in their cloud-based hosted environments and servers.

51. Defendants did not obtain Plaintiff's consent before disclosing or disseminating her biometric data to third-party "authorized subcontractors."

52. Defendants did not inform Plaintiff in writing of the specific limited purpose(s) or length of time for which they collected, obtained, stored, used and/or disclosed her biometric data.

53. Plaintiff has never seen, been able to access, or been informed of any publicly available biometric data retention policy or guidelines developed by Defendants, nor has she ever

seen, been able to access, or been informed of whether Defendants would ever permanently delete her biometric data.

54. Plaintiff has never been provided with, nor ever signed, a written release allowing any Defendant to collect, obtain, store, use, and/or disclose her biometric data.

55. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendants' multiple violations of BIPA alleged herein.

56. No amount of time or money can compensate Plaintiff if her biometric data is or has been compromised by the lax procedures through which Defendants collect, obtain, store, uses, and disclose Plaintiff's and other similarly-situated workers' biometric data. Moreover, Plaintiff would not have provided her biometric data to Defendants if she had known that they would retain such information for an indefinite period of time without her consent.

57. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act").

58. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, she seeks statutory damages under BIPA as compensation for the injuries caused by Defendants. *Rosenbach*, 2019 IL 123186, ¶ 40.

CLASS ALLEGATIONS

59. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS § 5/2-801, Plaintiff brings claims on her own behalf and as a representative of all other similarly-situated individuals pursuant to BIPA, 740 ILCS § 14/1, *et seq.*, to recover statutory penalties, prejudgment interest,

attorneys' fees and costs, and other damages owed. Specifically, Plaintiff, on behalf of herself and the putative class, alleges—as discussed *supra*, the following:

a. Defendants at least negligently, if not recklessly and/or intentionally, violated § 15(a) of BIPA as to Plaintiff and the putative class;

b. Defendants at least negligently, if not recklessly and/or intentionally, violated § 15(b) of BIPA as to Plaintiff and the putative class; and

c. Defendants at least negligently, if not recklessly and/or intentionally, violated § 15(d) of BIPA as to Plaintiff and the putative class.

60. Plaintiff seeks class certification under the Illinois Code of Civil Procedure, 735 ILCS § 5/2-801 for the following class of similarly-situated individuals under BIPA:

> All individuals who had their biometric identifier(s) and/or biometric information collected, captured, received, obtained, maintained, stored, or disclosed by Defendants in the State of Illinois during the applicable statutory period.

61. This action is properly maintained as a class action under 735 ILCS § 5/2-801 because:

a. The class is so numerous that joinder of all members is impracticable;

b. There are questions of law or fact that are common to the class;

c. The claims of Plaintiff are typical of the claims of the class; and

d. Plaintiff will fairly and adequately protect the interests of the class.

Numerosity

62. The total number of putative class members exceeds 2,000 individuals. The exact number of class members can easily be determined from Defendants' records.

Commonality

63. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendants' failure to comply with BIPA. The common questions of law and fact

include, but are not limited to the following:

a. Whether Defendants collected, captured, or otherwise obtained Plaintiff's and the Class members' biometric identifiers or biometric information;

b. Whether Defendants properly informed Plaintiff and the Class members of its purposes for collecting, obtaining, using, storing, and disclosing their biometric identifiers or biometric information;

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

d. Whether Defendants have disclosed or re-disclosed Plaintiff's and the Class members' biometric identifiers or biometric information;

e. Whether Defendants have sold, leased, traded, or otherwise profited from Plaintiff's and the Class members' biometric identifiers or biometric information;

f. Whether Defendants 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 with the individual, whichever occurs first;

g. Whether Defendants used Plaintiff's and the Class members' biometric identifiers to identify them;

h. Whether Defendants' violations of BIPA have raised a material risk that Plaintiff's and the putative Class members' biometric identifiers and/or biometric information will be unlawfully accessed by third parties;

i. Whether Defendants' violations of BIPA were committed negligently; and

j. Whether Defendants' violations of BIPA were committed intentionally and/or recklessly.

64. Plaintiff anticipates that Defendants will raise defenses that are common to the class.

Adequacy

65. Plaintiff will fairly and adequately protect the interests of all members of the Class,

and there are no known conflicts of interest between Plaintiff and the Class members. Plaintiff, moreover, has retained experienced counsel who are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

66. The claims asserted by Plaintiff are typical of the class members she seeks to represent. Plaintiff has the same interests and suffers from the same unlawful practices as the Class members.

67. There are no other Class members who have an interest individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim. However, if any such class member should become known, he or she can "opt out" of this action pursuant to 735 ILCS § 5/2-801.

Predominance and Superiority

68. The common questions identified above predominate over any individual issues. 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 would make it difficult for individual class members to vindicate their claims.

69. 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 Defendants 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.

FIRST CAUSE OF ACTION
Violation of 740 ILCS § 14/15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

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

71. 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).

72. Defendants failed to comply with these BIPA mandates.

73. Each Defendant qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

74. Plaintiff and the Class members are individuals who have had their "biometric identifiers" collected by Defendants (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

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

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

77. Defendants lack retention schedules and guidelines for permanently destroying Plaintiff's and the Class members' biometric data and has 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 each company.

78. On behalf of herself 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 Defendants 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 Plaintiff and each Class member who suffered a willful and/or reckless violation of BIPA Section 15(a) pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for Plaintiff and each Class member who suffered a negligent violation of BIPA Section 15(a) 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 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

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

80. BIPA requires companies to obtain informed written consent from individuals 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).

81. Defendants failed to comply with these BIPA mandates.

82. Each Defendant qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

83. Plaintiff and the Class members are individuals who have had their "biometric identifiers" collected by Defendants (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

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

85. Defendants systematically and automatically collected, obtained, 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).

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

87. By collecting, obtaining, using, and storing Plaintiff's and Class members' biometric identifiers and biometric information as described herein, Defendants violated Plaintiff's

and the Class's rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq*.

88. On behalf of herself 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 Defendants 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 Plaintiff and each Class member who suffered a willful and/or reckless violation of BIPA Section 15(b) pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for Plaintiff and each Class member who suffered a negligent violation of BIPA Section 15(b) 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).

THIRD CAUSE OF ACTION
Violation of 740 ILCS § 14/15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

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

90. BIPA prohibits private entities from disclosing a person's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS § 14/15(d)(1).

91. Defendants failed to comply with this BIPA mandate.

92. Each Defendant qualifies as "private entity" under BIPA. *See* 740 ILCS § 14/10.

93. Plaintiff and the Class members are individuals who have had their "biometric identifiers" collected by Defendants (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

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

95. Defendants systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff's biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS § 14/15(d)(1).

96. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class members' biometric identifiers and biometric information as described herein, Defendants violated Plaintiff's and the Class members' rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq.*

97. On behalf of herself 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 Defendants to comply with BIPA's requirements for the collection, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for Plaintiff and each Class member who suffered a willful and/or reckless violation of BIPA Section 15(d) pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for Plaintiff and each Class member who suffered a negligent violation of BIPA Section 15(d) 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 Faith Mendenhall 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 Faith Mendenhall as Class Representative, and appointing Stephan Zouras, LLP, as Class Counsel;

B. Declaring that Defendants' actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 to each Class member who suffered a reckless or intentional violation of BIPA Section 15(a) by Defendants pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each Class member who suffered a negligent violation of BIPA Section 15(a) by Defendants pursuant to 740 ILCS § 14/20(1);

D. Awarding statutory damages of $5,000 to each Class member who suffered a reckless or intentional violation of BIPA Section 15(b) by Defendants pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each Class member who suffered a negligent violation of BIPA Section 15(b) by Defendants pursuant to 740 ILCS § 14/20(1);

E. Awarding statutory damages of $5,000 to each Class member who suffered a reckless or intentional violation of BIPA Section 15(d) by Defendants pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each Class member who suffered a negligent violation of BIPA Section 15(d) by Defendants pursuant to 740 ILCS § 14/20(1);

F. Declaring that Defendants' actions, as set forth above, were intentional or reckless;

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

H. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3);

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

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

Date: February 16, 2024

Respectfully Submitted,

/s/ Ryan F. Stephan

Ryan F. Stephan
James B. Zouras
Teresa Becvar
STEPHAN ZOURAS, LLP
222 W. Adams St., Suite 2020
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com

jzouras@stephanzouras.com
tbecvar@stephanzouras.com
Firm ID: 43734

ATTORNEYS FOR PLAINTIFF

ClassAction.org
