12-Person Jury

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

CHARLENE FIGUEROA and JERMAINE BURTON, individually and on behalf of all others similarly situated,	)	
Plaintiffs,	)	**Case No.** 2019CH00744
v.	)	
KRONOS INCORPORATED,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Charlene Figueroa and Jermaine Burton ("Plaintiffs"), by and through their attorneys, individually and on behalf of all others similarly situated (the "Class"), bring the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against Kronos, Inc. ("Defendant"), its subsidiaries and affiliates, to redress and curtail Defendant's unlawful collection, use, storage, and disclosure of Plaintiffs' sensitive biometric data. Plaintiffs allege as follows upon personal knowledge as to themselves, their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys.

NATURE OF THE ACTION

1. Defendant Kronos Inc. ("Kronos") is a leading provider of human resource management software and services that's best known for helping hundreds of thousands of businesses track employee time and process payroll. In Illinois alone, Kronos provides timekeeping systems to thousands of employers including Mariano's, Chicago Lakeshore

Hospital, Smith Senior Living, Southwest Airlines, Speedway, NFI Industries and Con-Tech Lighting.

2. To help make employee time and attendance tracking more accurate, Kronos encourages its customers to use biometric-based time clocks, which use an employee's biometrics to punch in and out of work, instead of key fobs, identification numbers, or cards.

3. Unlike ID badges or time cards – which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with each employee. This exposes employees who are required to use Kronos devices as a condition of their employment to serious and irreversible privacy risks.

4. 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.

5. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregards the statutorily protected privacy rights of Illinois citizens and unlawfully collects, stores, disseminates, and uses their biometric data in violation of BIPA. Specifically, Defendant violated and continues to violate BIPA because it did not and continues not to:

a. Properly inform Plaintiffs and others similarly situated in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, disseminated and used, as required by BIPA;

b. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiffs' and other similarly-situated individuals' fingerprints, as required by BIPA; and

c. Receive a written release from Plaintiffs and others similarly situated to collect, store, disseminate or otherwise use their fingerprints, as required by BIPA.

6. Accordingly, this Complaint seeks an Order: (1) declaring that Defendant's conduct violates BIPA; (2) requiring Defendant to cease the unlawful activities discussed herein; and (3) awarding liquidated damages to Plaintiffs and the proposed class.

PARTIES

7. Plaintiff Charlene Figueroa is a natural person and a citizen in the State of Illinois.

8. Plaintiff Jermaine Burton is a natural person and citizen of the State of Illinois.

9. Defendant Kronos, Inc. is a corporation organized and existing under the laws of the State of Massachusetts. It is a registered with the Illinois Secretary of State and conducts business in Illinois, including in Cook County.

JURISDICTION AND VENUE

10. This Court has jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 because it conducts business transactions in Illinois, committed statutory violations and tortious acts in Illinois, and is registered to conduct business in Illinois.

11. Venue is proper in Cook County because Defendant is authorized to conduct business in this State, Defendant conducts business transactions in Cook County, and Defendant committed the statutory violations alleged herein in Cook County and throughout Illinois.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

12. Major national corporations started using Chicago and other locations in Illinois in the early 2000s 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.

13. 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. The bankruptcy was alarming to the Illinois legislature because there was suddenly a serious risk that millions of fingerprint records – which, similar to 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 the scanners were not 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.

14. 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.

15. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party 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.

16. 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, stored and used;

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.

See 740 ILCS 14/15(b).

17. 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.

18. 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. *Id.*

19. BIPA also establishes standards for how companies must handle Illinois citizens' biometric identifiers and biometric information. *See, e.g.,* 740 ILCS 14/15(c)-(d). For example, 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).

20. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information (740 ILCS 14/15(c)) and 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. The Illinois legislature enacted BIPA 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. Biometrics are biologically unique to the individual and, once compromised, an individual is at heightened risk for identity theft and left without any recourse. Biometric data, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

22. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored 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 disseminate biometrics and creates a private right of action for lack of statutory compliance.

II. Defendant Violates the Biometric Information Privacy Act.

23. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had experimented using employees' biometric data as an authentication method stopped doing so.

24. However, Defendant failed to take note of the shift in Illinois law governing the collection and use of biometric data. As a result, Defendant continues to collect, store, use, and disseminate Illinois employees' biometric data in violation of BIPA.

25. Specifically, when an employee first begins work at a company that uses one of Kronos' biometric devices, they are required to have their fingerprint or palm print scanned in order to enroll them in the Kronos database.

26. Unfortunately, Kronos fails to inform these employees that Kronos is collecting, storing or using their sensitive biometric data, the extent of the purposes for which it collects their sensitive biometric data, or to whom the data is disclosed, if at all.

27. In those instances, Kronos similarly fails to inform the employees that Kronos is collecting, storing, or using their sensitive biometric data, the extent of the purposes for which it collects their sensitive biometric data, or to whom the data is disclosed, if it all.

28. Kronos, up until recently, failed to provide employees with a written, publicly-available policy identifying its retention schedule and guidelines for permanently destroying employees' biometric data when the initial purpose for collecting or obtaining their biometrics is no longer relevant, as required by BIPA. Setting aside that Kronos has collected, stored, and used employees' biometric data for years without such a policy, the publishing of the recent policy on its website is also problematic. As described above, most employees don't know they are interacting with Kronos when they have their biometrics scanned by their employer's Kronos devices, let alone providing it their biometric data. As such, they'd have no reason to affirmatively seek out Kronos' website and search for its biometric data policies.

29. In addition, Kronos profits from the use of employees' biometric data. For instance, Kronos markets its biometric time clocks to employers as superior options to traditional time clocks, which can be deceived by "buddy punching" – where one employee punches in to or out of a time clock for another (absent) employee. By marketing its clocks in this manner, Kronos obtains a competitive advantage over other time clock companies and secures profits from its use of biometric data, all while failing to comply with the minimum requirements for handling employees' biometric data established by BIPA.

30. The Pay by Touch bankruptcy, which triggered the passage of BIPA, highlights why such conduct – where individuals are aware that they are providing a fingerprint but are not aware 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 data such as a fingerprint or data derived therefrom, who exactly is collecting their biometric data, where it will be transmitted, for what purposes it will be transmitted, and for how long.

31. Remarkably, Defendant has created the same situation that Pay by Touch did by assembling a database of biometric data through broadly deployed fingerprint scanners, but failed to comply with the law specifically designed to protect individuals whose biometrics are collected in these circumstances. Defendant disregards these obligations and Illinois employees' statutory rights and instead unlawfully collects, stores, uses, and disseminates employees' biometric identifiers and information without ever receiving the individual's informed written consent required by BIPA.

32. Upon information and belief, Defendant lacks retention schedules and guidelines for permanently destroying Plaintiffs' and other similarly-situated individuals' biometric data and has not and will not destroy Plaintiffs' and other similarly-situated individuals' 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. Kronos's publicly-available policies related to biometric data are not only tardy but also insufficient, placing the onus on employers to direct Kronos to destroy biometric data.

33. Plaintiffs and others similarly situated are not told whether and to whom Defendant currently discloses their biometric data, or what might happen to their biometric data in the event of a merger or a bankruptcy.

34. By and through the actions detailed above, Defendant disregarded Plaintiffs' and other similarly-situated individuals' legal rights in violation of BIPA.

III. Plaintiff Charlene Figueroa's Experience.

35. Plaintiff Charlene Figueroa was hired by Tony's Finer Foods Enterprises Inc. d/b/a Tony's Fresh Market on March 8, 2017 and was an hourly employee until September 17, 2018. As a condition of employment, Figueroa was required to scan her fingerprints using a Kronos device so her employer could track her time.

36. Kronos subsequently stored Figueroa's fingerprint data in its employee database(s).

37. Figueroa was required to scan her fingerprint on a Kronos device each time she clocked in for work and clocked out of work.

38. Figueroa was also required to scan her fingerprint on a Kronos device each time she clocked in and out for lunch.

39. Figueroa has never been informed of the specific limited purposes or length of time for which Defendant collected, stored, used, and/or disseminated her biometric data.

40. Figueroa has never been informed of any biometric data retention policy developed by Defendant, nor has she ever been informed whether Defendant will ever permanently delete her biometric data.

41. Figueroa has never been provided with nor ever signed a written release allowing Defendant to collect, store, use or disseminate her biometric data.

42. Figueroa has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA alleged herein.

43. No amount of time or money can compensate Figueroa if her biometric data is compromised by the lax procedures through which Defendant captured, stored, used, and disseminated her and other similarly-situated individuals' biometrics. Moreover, Figueroa would not have provided her biometric data to Defendant if she had known that they would retain such information for an indefinite period of time without her consent.

44. A showing of actual damages is not necessary in order to state a claim under BIPA. Nonetheless, Figueroa has been aggrieved because she suffered an injury-in-fact based on Defendant's violations of her legal rights. Defendant intentionally interfered with Figueroa's right to control her own sensitive biometric data. Additionally, Figueroa suffered an invasion of a legally protected interest when Defendant secured her personal and private biometric data at a time when it had no right to do so, a gross invasion of her right to privacy. BIPA protects employees like Figueroa from this precise conduct. Defendant had no lawful right to secure this data or share it with third parties absent a specific legislative license to do so.

45. Figueroa also suffered an injury in fact because Defendant improperly disseminated her biometric identifiers and/or biometric information to third parties, including but not limited to third parties that hosted the biometric data in their data centers, in violation of BIPA.

46. Finally, as a result of Defendant's conduct, Figueroa has experienced personal injury in the form of mental anguish. For example, Figueroa experiences mental anguish and injury when contemplating what would happen to her biometric data if Defendant went bankrupt, whether Defendant will ever delete her biometric information, and whether (and to whom) Defendant would share her biometric information.

47. Figueroa has plausibly inferred actual and ongoing harm in the form of monetary damages for the value of the collection and retention of her biometric data; in the form of monetary damages by not obtaining additional compensation as a result of being denied access to material information about Defendant's policies and practices; in the form of the unauthorized disclosure of her confidential biometric data to third parties; in the form of interference with her right to control her confidential biometric data; and, in the form of the continuous and ongoing exposure to substantial and irreversible loss of privacy.

48. As Figueroa 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 Defendant.

IV. Plaintiff Jermaine Burton's Experience.

49. Plaintiff Jermaine Burton worked for BWAY from January through April 2017 at its facility on Kilbourne in Chicago, Illinois. As a condition of employment, Burton was required to scan his fingerprints using a Kronos device so his employer could track his time.

50. Kronos subsequently stored Burton's fingerprint data in its employee database(s).

51. Burton was required to scan his fingerprint on a Kronos device each time he clocked in for work and clocked out of work.

52. Burton has never been informed of the specific limited purposes or length of time for which Defendant collected, stored, used, and/or disseminated his biometric data.

53. Burton has never been informed of any biometric data retention policy developed by Defendant, nor has he ever been informed whether Defendant will ever permanently delete his biometric data.

54. Burton has never been provided with nor ever signed a written release allowing Defendant to collect, store, use or disseminate his biometric data.

55. Burton has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA alleged herein.

56. No amount of time or money can compensate Burton if his biometric data is compromised by the lax procedures through which Defendant captured, stored, used, and disseminated her and other similarly-situated individuals' biometrics. Moreover, Burton would not have provided his biometric data to Defendant if he had known that they would retain such information for an indefinite period of time without his consent.

57. A showing of actual damages is not necessary in order to state a claim under BIPA. Nonetheless, Burton has been aggrieved because he suffered an injury-in-fact based on Defendant's violations of his legal rights. Defendant intentionally interfered with Burton's right to control his own sensitive biometric data. Additionally, Burton suffered an invasion of a legally protected interest when Defendant secured his personal and private biometric data at a time when it had no right to do so, a gross invasion of his right to privacy. BIPA protects employees like Burton from this precise conduct.

58. Burton has plausibly inferred actual and ongoing harm in the form of monetary damages for the value of the collection and retention of his biometric data; in the form of monetary damages by not obtaining additional compensation as a result of being denied access to material information about Defendant's policies and practices; in the form of interference with his right to control his confidential biometric data; and, in the form of the continuous and ongoing exposure to substantial and irreversible loss of privacy.

59. As Burton is not required to allege or prove actual damages in order to state a claim under BIPA, he seeks statutory damages under BIPA as compensation for the injuries caused by Defendant.

CLASS ALLEGATIONS

60. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS 5/2-801, Plaintiffs bring claims on their own behalf and as representatives 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.

61. Plaintiffs seek class certification under the Illinois Code of Civil Procedure, 735 ILCS 5/2-801 for the following class of similarly-situated employees under BIPA:

> All individuals working in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by Defendant during the applicable statutory period.

62. 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 the Plaintiffs are typical of the claims of the class; and,

D. The Plaintiffs will fairly and adequately protect the interests of the class.

Numerosity

63. The total number of putative class members exceeds fifty (50) individuals. The exact number of class members can easily be determined from Kronos' records.

Commonality

64. There is a well-defined commonality of interest in the substantial questions of law

and fact concerning and affecting the Class in that Plaintiffs and all members of the Class have been harmed by Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether Defendant collected, captured or otherwise obtained Plaintiffs' biometric identifiers or biometric information;

B. Whether Defendant properly informed Plaintiffs 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 Plaintiffs' biometric identifiers or biometric information;

D. Whether Defendant disclosed or re-disclosed Plaintiffs' biometric identifiers or biometric information;

E. Whether Defendant sold, leased, traded, or otherwise profited from Plaintiffs' biometric identifiers or biometric information;

F. 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 with the individual, whichever occurs first;

G. Whether Defendant complies with any such written policy (if one exists);

H. Whether Defendant used Plaintiffs' fingerprints to identify them;

I. Whether Defendant's violations of BIPA have raised a material risk that Plaintiffs' biometric data will be unlawfully accessed by third parties;

J. Whether the violations of BIPA were committed negligently; and

K. Whether the violations of BIPA were committed willfully.

65. Plaintiffs anticipate that Defendant will raise defenses that are common to the class.

Adequacy

66. Plaintiffs will fairly and adequately protect the interests of all members of the class,

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

Typicality

67. The claims asserted by Plaintiffs are typical of the class members they seek to represent. Plaintiffs have the same interests and suffer from the same unlawful practices as the class members.

68. Upon information and belief, 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 and the difficulties involved in bringing individual litigation against one's employer. However, if any such class member should become known, she or she can "opt out" of this action pursuant to 735 ILCS 5/2-801.

Predominance and Superiority

69. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. 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.

70. 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 Defendant 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 14/1, *et seq.*
(On Behalf of Plaintiffs and the Class)

71. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

72. 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).

73. Furthermore, 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).

74. Defendant fails to comply with these BIPA mandates.

75. Defendant Kronos is a corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

76. Plaintiffs are both individuals who had their "biometric identifiers" collected by Defendant (in the form of their fingerprints), as explained in detail in Sections III and IV, *supra*. *See* 740 ILCS 14/10.

77. Information based upon Plaintiffs' biometric identifiers was used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

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

79. Upon information and belief, Defendant systematically disclosed Plaintiffs' biometric identifiers and biometric information to other currently unknown third parties, which hosted the biometric data in their data centers.

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

81. Defendant did not 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).

82. By collecting, storing, and using Plaintiffs' and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiffs' 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.*

83. Upon information and belief, Defendant lacks retention schedules and guidelines for permanently destroying Plaintiffs' and the Class's biometric data and have not and will not destroy Plaintiffs' 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.

84. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring 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, Plaintiffs Charlene Figueroa and Jermaine Burton respectfully request that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs Charlene Figueroa and Jermaine Burton as Class Representatives, and appointing their counsel as Class Counsel;

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

C. Awarding 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);

D. Declaring that Defendant's actions, as set forth above, were willful;

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

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

G. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable;

H. Provide such further relief as the Court deems just and equitable.

JURY TRIAL

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

Date: January 18, 2019

Respectfully Submitted,

/s/ James B. Zouras

James B. Zouras
Ryan F. Stephan
Andrew C. Ficzko
Haley R. Jenkins
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza
Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
Firm ID: 43734
jzouras@stephanzouras.com

rstephan@stephanzouras.com
aficzko@stephanzouras.com
hjenkins@stephanzouras.com

Benjamin H. Richman
J. Eli Wade-Scott
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
312.589.6370
312.589.6378 *f*
Firm ID: 62075
brichman@edelson.com
ewadescott@edelson.com

David Fish
John Kunze
THE FISH LAW FIRM, P.C.
200 East Fifth Avenue, Suite 123
Naperville, Illinois 60563
630.355.7590
630.778.0400 *f*
Firm ID: 44086

dfish@fishlawfirm.com
jkunze@fishlawfirm.com