YES

EXHIBITS

CASE NO. 2018CH09277

DATE: 7/24/2018

CASE TYPE: Class Action

PAGE COUNT: 24

CASE NOTE

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

JENNIFER CHATMAN, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No.** 2018CH09277
v.	)	
EUROMARKET DESIGNS, INC. d/b/a CRATE & BARREL,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Jennifer Chatman ("Chatman" or "Plaintiff"), by and through her attorneys, individually and on behalf of all others similarly situated (the "Class"), brings the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, Euromarket Designs, Inc., d/b/a Crate & Barrel ("C & B" or "Defendant"), its subsidiaries and affiliates, to redress and curtail Defendant's unlawful collection, use, storage, and disclosure of Plaintiff's sensitive biometric data. Plaintiff alleges as follows upon personal knowledge as to herself, her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. Defendant C & B is a retail store specializing in housewares, furniture, and home accessories.

2. When C & B hires an employee, he or she is enrolled in its employee database. Defendant uses the employee database to monitor the time worked by C & B's hourly employees.

3. While many employers use conventional methods for tracking time worked (such as ID badge swipes or punch clocks), C & B's employees are required to have their fingerprints scanned by a biometric timekeeping device.

4. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as Defendant – and financial institutions have incorporated biometric applications into their workplace in the form of biometric timeclocks, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

5. 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 C & B's employees 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 – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches – employees have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

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

7. A black market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian

citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than $8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), *available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

8. 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 and store Illinois citizens' biometrics, such as fingerprints.

9. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregards C & B employees' statutorily protected privacy rights and unlawfully collects, stores, disseminates, and use its employees' biometric data in violation of BIPA. Specifically, Defendant has violated and continues to violate BIPA because it did not and continues not to:

a. Properly inform Plaintiff 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 Plaintiff's and other similarly-situated individuals' fingerprints, as required by BIPA; and

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

10. Plaintiff and other similarly-situated individuals are aggrieved because they were not: (1) informed in writing of the purpose and length of time for which their fingerprints were

being collected, stored, disseminated and used; (2) provided a publicly available retention schedule or guidelines for permanent destruction of the biometric data; and (3) provided (nor did they execute) a written release, as required by BIPA.

11. Upon information and belief, C & B improperly discloses its employees' fingerprint data to at least one other, currently unknown third party, including, but not limited to third parties that host biometric data in their data center(s).

12. Upon information and belief, Defendant improperly discloses its employees' fingerprint data to a currently unknown third-party vendor for payroll purposes.

13. Upon information and belief, Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and have not and will not destroy their biometric data as required by BIPA.

14. Plaintiff and others similarly situated are aggrieved by Defendant's failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the employee's last interactions with the company.

15. Plaintiff and others similarly situated have suffered an injury in fact based on Defendant's improper disclosures to any third parties.

16. Plaintiff and others similarly situated have suffered an injury in fact based on Defendant's violations of their legal rights.

17. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties. The Illinois Attorney General has just ranked identity theft as the top scam targeting Illinois residents. (*See* Exhibit A).

18. Employees have a proprietary right to control their biometric information. In failing to comply with the requirements of BIPA, employers intentionally interfere with each employees' right of possession and control over their valuable, unique, and permanent biometric data.

19. Defendant is directly liable for, and had actual knowledge of, the BIPA violations alleged herein.

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

PARTIES

21. Plaintiff Jennifer Chatman is a natural person and a citizen in the State of Illinois.

22. Defendant C & B is a corporation organized and existing under the laws of the State of Illinois, with its principle place of business in Northbrook, Illinois. C & B is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

JURISDICTION AND VENUE

23. 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.

24. Venue is proper in Cook County because Defendant conducts business in Cook County and committed the statutory violations alleged herein in Cook County.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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:

a. Informs the subject in writing that a biometric identifier or biometric information is being collected or stored;

b. 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

c. Receives a written release executed by the subject of the biometric identifier or biometric information."

See 740 ILCS 14/15(b).

30. 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.

31. 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.*

32. 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 or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

33. 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).

34. 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.

35. 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.

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

II. Defendant Violates the Biometric Information Privacy Act.

37. 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.

38. 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 employees' biometric data in violation of BIPA.

39. Specifically, when employees are hired, C & B requires them to have their fingerprints scanned to enroll them in its employee database.

40. C & B uses an employee time tracking system that requires employees to use their fingerprint as a means of authentication. Unlike a traditional timeclock, employees have to use their fingerprints to "punch" in and out of work.

41. Upon information and belief, Defendant fails to inform its workers that it discloses their fingerprint data to third-party payroll vendors.

42. Upon information and belief, C & B fails to inform its employees that it discloses their fingerprint data to any third-party vendors which host the biometric data in their data centers; fails to inform its employees of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from employees before collecting their fingerprints.

43. Furthermore, Defendant fails to provide employees with a written, publicly available policy identifying its retention schedule and guidelines for permanently destroying employees' fingerprints when the initial purpose for collecting or obtaining their fingerprints is no longer relevant, as required by BIPA.

44. 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 identifiers such as a fingerprint, who exactly is collecting their biometric data, where it will be transmitted, for what purposes it will be transmitted, and for how long. Defendant disregards these obligations and their 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.

45. Upon information and belief, Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and have not and will not destroy Plaintiff's 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 employee's last interaction with the company.

46. C & B's employees are not told what might happen to their biometric data if and when it merges with another company or worse, if and when Defendant's business folds or when the other third parties' that have received biometric data business folds.

47. Since Defendant neither publishes a BIPA-mandated data retention policy nor discloses the purposes for its collection of biometric data, C & B's employees have no idea whether Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and others similarly situated are not told to whom Defendant currently discloses their biometric data to, or what might happen to their biometric data in the event of a merger or a bankruptcy.

48. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

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

III. Plaintiff Jennifer Chatman's Experience

50. Plaintiff Jennifer Chatman worked as a Sales Team Lead for Defendant C & B, at its former location at 646 North Michigan Avenue, Chicago, IL 60611. Chatman worked for C & B from October 2010 to June 12, 2017.

51. As a condition of employment, Chatman was required to scan her fingerprint so C & B could use it as an authentication method to track her time.

52. C & B subsequently stored Chatman's fingerprint data in its database(s) and disseminates Chatman's fingerprint data to currently-unknown third parties, including but not limited to those that host biometric data in their data center(s).

53. Chatman was required to scan her fingerprint each time she began and ended her workday.

54. Chatman 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.

55. Chatman 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.

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

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

58. No amount of time or money can compensate Chatman 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, and Chatman would not have provided her biometric data to either Defendant if she had known that they would retain such information for an indefinite period of time without her consent.

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

60. Chatman's biometric information is economically valuable, and such value will increase as the commercialization of biometrics continues to grow. As such, Chatman was not sufficiently compensated by Defendant for its retention and use of her and other similarly-situated employees' biometric data. Chatman would not have agreed to work for C & B for the compensation she received if she had known that Defendant would retain her biometric data indefinitely.

61. Chatman also suffered an informational injury because Defendant failed to provide her with information to which she was entitled by statute. Through BIPA, the Illinois legislature

has created a right: an employee's right to receive certain information prior to an employer securing their highly personal, private and proprietary biometric data – and an injury – not receiving this extremely critical information.

62. Chatman 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 any other third party that hosted the biometric data in their data centers, in violation of BIPA.

63. Pursuant to 740 ILCS 14/15(b), Chatman was entitled to receive certain information prior to Defendant securing her biometric data; namely, information advising her of the specific limited purpose(s) and length of time for which Defendant collects, stores, uses and disseminates her private biometric data; information regarding Defendant's biometric retention policy; and, a written release allowing Defendant to collect, store, use, and disseminate her private biometric data. By depriving Chatman of this information, Defendant injured her. *Public Citizen v. U.S. Department of Justice*, 491 U.S. 440, 449 (1989); *Federal Election Commission v. Akins*, 524 U.S. 11 (1998).

64. Finally, as a result of Defendant's conduct, Chatman has experienced personal injury in the form of mental anguish. For example, Chatman 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.

65. Chatman 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 and possess her confidential biometric data; and, in the form of the continuous and ongoing exposure to substantial and irreversible loss of privacy.

66. As Chatman 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.

CLASS ALLEGATIONS

67. 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.

68. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it first (1) informs the individual in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the individual in writing of the specific purpose and length of time 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.

69. Plaintiff seeks 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 for C & B in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by Defendant during the applicable statutory period.

70. 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 Plaintiff are typical of the claims of the class; and,

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

Numerosity

71. The total number of putative class members exceeds fifty (50) individuals. The exact number of class members can easily be determined from Defendant's payroll records.

Commonality

72. 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 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 Plaintiff's biometric identifiers or biometric information;

B. Whether Defendant properly informed Plaintiff of its purposes for collecting, using, and storing her biometric identifiers or biometric information;

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

D. Whether Defendant has disclosed or re-disclosed Plaintiff's biometric identifiers or biometric information;

E. Whether Defendant has sold, leased, traded, or otherwise profited from Plaintiff's 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 employee, whichever occurs first;

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

H. Whether Defendant used Plaintiff's fingerprints to identify her;

I. Whether Defendant's violations of BIPA have raised a material risk that Plaintiff's 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.

73. Plaintiff anticipates that Defendant will raise defenses that are common to the class.

Adequacy

74. 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 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

75. 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.

76. 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, he or she can "opt out" of this action pursuant to 735 ILCS 5/2-801.

Predominance and Superiority

77. 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.

78. 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 Plaintiff and the Class)

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

80. 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).

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

82. 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).

83. Defendant fails to comply with these BIPA mandates.

84. Defendant C & B is an Illinois corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

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

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

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

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

89. Defendant failed to inform Plaintiff in writing that her biometric identifiers and/or biometric information were being collected, stored, used, and disseminated, nor did Defendant inform Plaintiff in writing of the specific purpose and length of term for which her biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

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

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

92. Upon information and belief, Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and the Class's 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 employee's last interaction with the company.

93. These violations have raised a material risk that Plaintiff's and the Class's biometric data will be unlawfully accessed by third parties.

94. 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 Defendant to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each willful and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

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

96. Defendant owed Plaintiff and the Class a duty of reasonable care. Such duty required Defendant to exercise reasonable care in the collection and use of Plaintiff's and the Class's biometric data.

97. Additionally, C & B owed Plaintiff and the Class a heightened duty – under which it assumed a duty to act carefully and not put Plaintiff and the Class at undue risk of harm – because of the employment relationship of the parties.

98. Defendant breached its duty by failing to implement a BIPA-compliant biometric time tracking system with reasonable data security safeguards.

99. Specifically, Defendant breached its duty by failing to properly inform Plaintiff and the Class in writing of the specific purpose or length of time for which their fingerprints were being collected, stored, used, and disseminated.

100. Defendant also breached its duty by failing to provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and the Class's fingerprint data.

101. Upon information and belief, Defendant breached its duty because it lacks retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and have not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the employee's last interaction with the company.

102. These violations have raised a material risk that Plaintiff's and the Class's biometric data will be unlawfully accessed by third parties.

103. As a direct and proximate cause of Defendant's negligent misrepresentations, Plaintiff and the other Class members have suffered from diminution in the unique identifying value of their biometric information caused by Defendant's repeated dissemination and exposure of such information to multiple third parties, including data storage vendors, among others.

104. Defendant knew or should have known that its breach would cause Plaintiff and the other Class members to experience the foreseeable harms associated with the exposure of their biometrics to third parties, including the discontinuation of Plaintiff's and the Class member's exclusive possession and control of their biometrics and the accompanying loss of the unique identifying value of their biometrics.

105. Further, Defendant's breach of its duty proximately caused and continues to cause an invasion of Plaintiff's and the Class's privacy, an informational injury, and mental anguish, in addition to the statutory damage provided in BIPA.

106. Accordingly, Plaintiff seeks an order declaring that Defendant's conduct constitutes negligence and awarding Plaintiff and the Class damages in an amount to be calculated at trial.

PRAYER FOR RELIEF

Wherefore, Plaintiff Jennifer Chatman 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 Jennifer Chatman as Class Representative and appointing Stephan Zouras, LLP, 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, constitute negligence;

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

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

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

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

I. 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: July 24, 2018 Respectfully Submitted,

/s/ Haley R. Jenkins
Ryan F. Stephan
James B. Zouras
Haley R. Jenkins
STEPHAN ZOURAS, LLP
205 N. Michigan Avenue
Suite 2560
Chicago, Illinois 60601
312.233.1550
312.233.1560 *f*
Firm ID: 43734
hjenkins@stephanzouras.com

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on July 24, 2018, I filed the attached with the Clerk of the Court using the electronic filing system which will send such filing to all attorneys of record.

/s/ Haley R. Jenkins