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

LATRINA COTHRON, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No.** 2018CH15233
v.	)	
WHITE CASTLE FOOD PRODUCTS, LLC D/B/A WHITE CASTLE, and CROSS MATCH TECHNOLOGIES, INC.,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Latrina Cothron ("Cothron" 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, against White Castle Food Products, LLC and Cross Match Technologies, Inc., (Collectively "Defendants"), their subsidiaries and affiliates, to redress and curtail Defendants' 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 White Castle Food Products, LLC ("White Castle") is a food retailer that processes and distributes fast food products in retail stores and restaurants nationally.

2. Defendant Cross Match Technologies, INC. ("Crossmatch") is a technology company that provides software and hardware that tracks and monitors employees' biometric data to companies worldwide.

3. When White Castle hires an employee, he or she is enrolled in its DigitalPersona employee database using a scan of his or her fingerprint. White Castle uses the DigitalPersona employee database to distribute their employees' paystubs on a weekly basis.

4. While many employers use conventional methods for payroll (direct deposit or paper check), White Castle's employees are required to have their fingerprints scanned by a biometric device to retrieve their paystubs.

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

6. Unlike ID badges– which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with each employee. This exposes White Castle'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 or misuses – 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.

7. 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.

8. An illegal 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=.b3c70259fl38.

9. 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.

10. 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, store and use Illinois citizens' biometrics, such as fingerprints.

11. Notwithstanding the clear and unequivocal requirements of the law, Defendants disregard White Castle employees' statutorily protected privacy rights and unlawfully collect, store, disseminate, and use employees' biometric data in violation of BIPA. Specifically, each Defendant has violated and continues to violate BIPA because they did not and continue 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.

12. 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.

13. Upon information and belief, Defendant White Castle improperly discloses its employees' fingerprint data to at least one third-party, DigitalPersona, and likely others.

14. Upon information and belief, Defendants White Castle and Crossmatch improperly disclose White Castle employees' fingerprint data to other, currently unknown, third parties, including, but not limited to third parties that host biometric data in their data center(s).

15. Upon information and belief, each 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.

16. Plaintiff and others similarly situated are aggrieved by each 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.

17. Plaintiff and others similarly situated have suffered an injury in fact based on each Defendant's improper disclosures of their biometric data to third parties.

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

19. 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, e.g.*, Exhibit A).

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

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

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

PARTIES

23. Plaintiff Latrina Cothron is a natural person and a citizen in the State of Illinois.

24. Defendant White Castle is an Ohio corporation that is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

25. Defendant Crossmatch is a corporation existing under the laws of the State of Illinois, that is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

JURISDICTION AND VENUE

26. This Court has jurisdiction over Defendants pursuant to 735 ILCS 5/2-209 because they conduct business transactions in Illinois, committed statutory violations and tortious acts in Illinois, and are registered to conduct business in Illinois.

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

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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, stored and used;

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).

33. 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.

34. 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*.

35. 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).

36. 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).

37. 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.

38. 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.

39. 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. Defendants Violate the Biometric Information Privacy Act.

40. 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.

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

42. Specifically, when employees are hired by White Castle, they are required to have their fingerprints scanned to enroll them in its DigitalPersona employee database(s).

43. White Castle uses and has used employee software supplied by Crossmatch that requires employees to use their fingerprint as a means of authentication. Per the company's policy, all White Castle employees were required to use their fingerprints to access their weekly paystubs.

44. Upon information and belief, White Castle failed and continues to fail to inform its employees that it discloses or disclosed their fingerprint data to at least one third party: DigitalPersona, and likely others; fails to inform its employees that it discloses their fingerprint data to other, currently unknown, third parties, 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.

45. Upon information and belief, White Castle fails to inform their employees that it discloses their fingerprint data to other, currently unknown, third parties, which host the biometric data in their data centers; fails to inform White Castle employees of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from White Castle employees before collecting their fingerprints.

46. Furthermore, each Defendant fails to provide employees with a written, publicly available policy identifying their 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.

47. 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. Each Defendant disregards these obligations and White Castle employees' statutory rights and instead

unlawfully collect, store, use, and disseminate employees' biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

48. Upon information and belief, each 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 individual's last interaction with each company.

49. White Castle employees are not told what might happen to their biometric data if and when any Defendant merges with another company or worse, if and when any Defendant's business folds, or when the other third parties that have received their biometric data businesses fold.

50. Since Defendants neither publish BIPA-mandated data retention policies nor disclose the purposes for their collection of biometric data, White Castle employees have no idea whether any Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and others similarly situated individuals are not told to whom any Defendant currently discloses their biometric data to, or what might happen to their biometric data in the event of a merger or a bankruptcy.

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

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

III. Plaintiff Latrina Cothron's Experience

53. Plaintiff Latrina Cothron was hired by White Castle in 2004 and is currently working as a manager.

54. As a condition of employment, Cothron was required to scan her fingerprints so White Castle could use it as an authentication method for Plaintiff to access the computer as a manager and to access to her paystubs as an hourly employee.

55. White Castle subsequently stored Cothron's fingerprint data in its DigitalPersona employee database(s).

56. Cothron was required to scan her fingerprint each time she accessed a White Castle computer.

57. Cothron was also required to scan her fingerprint each time she accessed her paystub.

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

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

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

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

62. No amount of time or money can compensate Cothron if her biometric data is compromised by the lax procedures through which each Defendant captured, stored, used, and

disseminated her and other similarly-situated individuals' biometrics. Moreover, Cothron would not have provided her biometric data to any Defendant if she had known that they would retain such information for an indefinite period of time without her consent.

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

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

65. Cothron also suffered an informational injury because each 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.

66. Cothron also suffered an injury in fact because each Defendant improperly disseminated her biometric identifiers and/or biometric information to third parties, including but not limited to DigitalPersona, and any other third party that hosted the biometric data in their data centers, in violation of BIPA.

67. Pursuant to 740 ILCS 14/15(b), Cothron was entitled to receive certain information prior to Defendants securing her biometric data; namely, information advising her of the specific limited purpose(s) and length of time for which each Defendant to collect, store, use and disseminate her private biometric data; information regarding each Defendant's biometric retention policy; and, a written release allowing each Defendant to collect, store, use, and disseminate her private biometric data. By depriving Cothron of this information, Defendants 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).

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

69. Cothron 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 Defendants' 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.

70. As Cothron 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.

CLASS ALLEGATIONS

71. 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.

72. 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.

73. 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 White Castle in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by any Defendant during the applicable statutory period.

74. 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

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

Commonality

76. 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 any Defendant collected, captured or otherwise obtained Plaintiff's biometric identifiers or biometric information;

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

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

E. Whether any Defendant has sold, leased, traded, or otherwise profited from Plaintiff's biometric identifiers or biometric information;

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

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

I. Whether any 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.

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

Adequacy

78. 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

79. 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.

80. 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

81. 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.

82. 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 14/1, *et seq.*
(On Behalf of Plaintiff and the Class)

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

84. 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).

85. 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).

86. 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).

87. Each Defendant fails to comply with these BIPA mandates.

88. Defendant White Castle is an Ohio corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

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

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

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

92. Each 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).

93. Upon information and belief, White Castle systematically disclosed Plaintiff's biometric identifiers and biometric information to at least one third party, DigitalPersona.

94. Upon information and belief, each 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.

95. No Defendant informed Plaintiff in writing that her biometric identifiers and/or biometric information were being collected, stored, used, and disseminated, nor did any 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).

96. No Defendant provides 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).

97. By collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, each 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*.

98. Upon information and belief, each Defendant 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 individual's last interaction with the company.

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

100. 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 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)

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

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

103. Additionally, White Castle 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.

104. Each Defendant breached its duties by failing to implement a BIPA-compliant biometric authentication system with reasonable data security safeguards.

105. Specifically, each Defendant breached its duties 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.

106. Defendants also breached their duties by failing to provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and the Class's fingerprint data.

107. Upon information and belief, each Defendant breached its duties 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 individual's last interaction with either company.

108. Upon information and belief, White Castle breached its duties because it systematically disclosed Plaintiff's biometric identifiers and biometric information to at least one third party: DigitalPersona.

109. Upon information and belief, each Defendant breached its duties because it systematically disclosed Plaintiff's biometric identifiers and biometric information to other, currently unknown, third parties, which hosted the biometric data in their data centers.

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

111. As a direct and proximate cause of each 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 Defendants' repeated dissemination and exposure of such information to third-parties, including DigitalPersona, and data storage vendors, among others.

112. Defendants knew or should have known that their breaches 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.

113. Further, each 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.

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

PRAYER FOR RELIEF

Wherefore, Plaintiff Latrina Cothron 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 Latrina Cothron 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 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 Defendants' actions, as set forth above, constitute negligence;

E. Declaring that Defendants' 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 Defendants 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; and,

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: December 6, 2018

Respectfully Submitted,

/s/ Andrew C. Ficzko

Ryan F. Stephan
Andrew C. Ficzko
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza
Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
Firm ID: 43734
Aficzko@stephanzouras.com

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on December 6, 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/ Andrew C. Ficzko