☐ YES ☑ NO

EXHIBITS

CASE NO. 2021 CH 10

DATE: 1/4/2021

CASE TYPE: Class Action

PAGE COUNT: 20

CASE NOTE

_____

_____

_____

12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
CHANCERY DIVISION

DEVONTE GRANT, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	CASE NO. 2021CH00010
v.	)	JURY TRIAL DEMANDED
BLOMMER CHOCOLATE COMPANY,	)	
Defendant.	)	

CLASS ACTION COMPLAINT & JURY DEMAND

Plaintiff Devonte Grant ("Plaintiff"), individually, and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant, Blommer Chocolate Company, ("Defendant"), to stop Defendant's capture, collection, use and storage of individuals' biometric identifiers and/or biometric information in violation of the Illinois Biometric Information Privacy Act ("BIPA") 740 ILCS 14/1 *et seq*., and to obtain redress for all persons injured by Defendant's conduct. Plaintiff alleges the following upon information and belief, except as to the allegations within Plaintiff's personal knowledge, and states as follows:

NATURE OF ACTION

1. Defendant, Blommer Chocolate Company, owns, operates and manages a factory at 600 W. Kinzie Street, Chicago, Illinois.

2. When Defendant hires a worker, including Plaintiff, he or she is enrolled in its employee database(s) using a scan of his or her fingerprint. Defendant uses the worker database(s) to monitor the time worked by its workers.

3. While many employers use conventional methods for tracking time worked (such as ID badges or punch clocks), Defendant's workers are required, as a condition of employment, 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's – and financial institutions have incorporated biometric applications into their workplace in the form of biometric timeclocks or authenticators, 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 – a fingerprint is a unique, permanent biometric identifier associated with each employee. This exposes Defendant's employees to serious and irreversible risks. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Clearview AI, Facebook/Cambridge Analytica, and Suprema 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* www.opm.gov/cybersecurity/cybersecurity-incidents.

7. 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 facial photographs – 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.

8. 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.tribunemedia.com/news/nation/rs-500-10-minutes-and0you-have-access-to-billion-aadhaar-details/523361.html.

9. In August 2019 it was widely reported that Suprema, a security company responsible for a web-based biometrics lock system that uses fingerprints and facial geometry scans in 1.5 million locations around the world, maintained biometric data and other personal information on a publicly accessible, unencrypted database. Major Breach Found in Biometrics System Used by Banks, UK police and Defence Firms, The Guardian (Aug. 14, 2019), available at https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

10. This practice has been criticized by lawmakers. Some states, including Illinois, have refused to comply with law enforcement's invasive requests. *State Denying Facial Recognition Requests*, Jacksonville Journal-Courier (July 9, 2019), *available at* https://www.myjournalcourier.com/news/article/State-denying-in-facial-recognition-requests-14081967.php.

11. 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.

12. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregarded Plaintiff's and other similarly-situated workers' statutorily protected rights and unlawfully collected, stored, disseminated, and used Plaintiff's and other similarly-situated workers' 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 Plaintiff and others similarly situated in writing of the specific purpose and length of time for which their fingerprints were being collected, stored, and used, as required by BIPA;

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

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

d. Obtain consent from Plaintiff and others similarly situated to disclose, redisclose, or otherwise disseminate their fingerprints to a third party as required by BIPA.

13. Accordingly, Plaintiff, on behalf of himself 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

14. Plaintiff Devonte Grant is, and has been at all relevant times, a resident and citizen of the State of Illinois and a resident of Cook County, Illinois.

15. Plaintiff Devonte Grant worked as a refinery operator at Defendant's facility located at 600 W. Kinzie Street in Chicago, Illinois in 2017, 2018 and 2019**.**

16. Since at least five years before the filing of this Complaint, Defendant Blommer Chocolate Company has been Delaware corporation registered with the Illinois Secretary of State to do business in Illinois.

17. Defendant owns, operates and manages the facility at 600 W. Kinzie Street in Chicago, Illinois.

18. Defendant manufactures chocolate and cocoa products at the facility located at 600 W. Kinzie Street in Chicago, Illinois.

19. Defendant transacts business in Cook County, Illinois.

20. Defendant transacts business with Cook County, Illinois businesses and residences.

21. Defendant employs Cook County, Illinois residents.

22. During the five years prior to the filing of this Complaint, Defendant captured, collected, stored and used the fingerprints of residents of Cook County and the State of Illinois without providing them the informed written consent required under BIPA.

23. During the five years prior to the filing of this Complaint, Defendant captured, collected, stored and used the fingerprints of residents of Cook County and the State of Illinois and failed to institute, maintain and adhere to a publicly-available retention schedule, in violation of BIPA.

24. Defendant is private entity as that term is defined under BIPA, 740 ILCS § 14/10.

JURISDICTION AND VENUE

25. This Court may assert personal jurisdiction over Defendant pursuant to 735 ILCS § 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendant is doing business within this State and because Plaintiff's claims arise out of Defendant's unlawful in-state actions, as Defendant captured, collected, stored, and used

Plaintiff's biometric identifiers and/or biometric information in this State.

26. Venue is proper in Cook County, Illinois because the transaction(s) that gave rise to Plaintiff's cause of action arose in Cook County, Illinois. Venue is also proper in this Court pursuant to 735 ILCS § 5/2-101 because Defendant does business in Cook County and, thus, resides there under 735 ILCS § 5/2-102. Further, venue is proper because the Plaintiff is resident of Cook County, Illinois.

SUBSTANTIVE ALLEGATIONS

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

28. In 2007, a biometrics company called Pay By Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records – which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections of Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

29. In 2008, following the 2007 bankruptcy of Pay by Touch, the Illinois Legislature passed BIPA, which contain detailed regulations and laws addressing the collection, use and retention of biometric information by private entities, such as Defendant.

30. The Illinois Legislature found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

31. BIPA defines "biometric identifiers" or "biometric information" as fingerprints, a scan of hand geometry, and any "information" based on such "identifiers" that is used to identify an individual. 740 ILCS § 14/10.

32. Illinois enacted BIPA to regulate entities that capture, collect, store and use biometric information.

33. The law is specifically designed to require a company that collects biometrics to meet certain conditions, prior to collecting biometric data in order to inform and protect the person whose biometrics it is taking for its own use, and requires signed, written consent attesting that the individual has been properly informed and has freely consented to biometrics collection.

34. Under BIPA, private entities may not collect, capture, purchase, receive through trade, or otherwise obtain a person's biometric identifier or biometric information unless they first:

a. Inform the person in writing that a biometric identifier or biometric information is being collected;

b. Inform the person in writing of the specific purpose and length of time for which a person's biometric identifier and/or biometric information is being captured, collected, stored, and used; and

c. Receive a written release executed by the subject of the biometric identifier or biometric information providing consent.

740 ILCS 14/15(b).

35. Section 15(a) of BIPA also requires that a private entity in possession of biometric identifiers and/or biometric information develop:

a. A written policy;

b. Available to the public;

c. Which establishes a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information;

d. Within three years of the individual's last interaction with the private entity, or when the purpose for collecting or obtaining the biometric identifiers and/or biometric information has been satisfied.

36. BIPA provides valuable rights, protections, and benefits to people in the State of Illinois. These requirements ensure that the environment for taking or collecting biometrics is not forced or coerced so that individuals are freely advised that by obtaining one's biometric data, the employer is capturing, extracting, creating and recording biometric data, and that individuals can monitor their biometric usage and history.

37. BIPA provides statutory damages if a company takes an individual's biometric information and invades an individual's rights by circumventing BIPA's preconditions and requirements.

38. To ensure compliance, BIPA provides that for a BIPA violation, the prevailing party may recover $1,000.00 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.

39. In the context of employment and work, BIPA requires express written consent, not only in order to capture or collect biometrics, but the company collecting, using and/or storing the fingerprint is required to obtain "informed written consent," in the form of "a release executed by an employee." Those formalized protections enable individuals to freely consent to the taking of their biometrics. (740 ILCS 14/10).

40. Defendant requires its workers to scan their fingers to "clock in" and "clock out" of work each day. Defendant does this using biometric timekeeping devices which capture, collect, store and use the workers' fingerprints. These fingerprint scans are distinctive identifiers of each individual and constitute biometric identifiers and information under BIPA.

41. Unlike ID cards or key codes – which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with the individual. Defendant's policies and action violate workers' substantive rights protected under BIPA and exposes Plaintiff and other workers to serious and irreversible risks.

42. The risks associated with a person's biometrics are considerable. Such information is more sensitive than a social security number, passport, birth certificate, etc. As such, Illinois' BIPA statute requires private entities to provide certain disclosures and obtain a written release

from individuals prior to collecting their biometric identifiers and/or biometric information. Accordingly, BIPA protects an individual's right to be informed with regard to the capture, collection, storage and use of their biometric information, allowing them to make more informed decisions as to the circumstances under which they agree to provide their biometric identifiers and/or biometric information.

43. Defendant's practice of collecting, capturing, storing, and/or using an individual's biometric information is unlawful under BIPA because such practices fail to satisfy each of the enumerated requirements described above, and therefore severely infringe on its workers' rights with regard to their biometric identifiers and information.

FACTS SPECIFIC TO PLAINTIFF

44. Plaintiff Devonte Grant worked as a refinery operator at Defendant's facility located at 600 W. Kinzie Street in Chicago, Illinois in 2017, 2018 and 2019**.**

45. When Plaintiff performed work for Defendant, Defendant collected, used and captured Plaintiff's and other workers' fingerprints and fingerprints scans. When Plaintiff performed work for Defendant, Defendant required individuals and workers, including Plaintiff, to provide Defendant with their fingerprints, and then, using biometrics, captured or converted Plaintiff's and other workers' and individuals' fingerprints as a means of identifying and tracking hours worked by the workers and individuals.

46. Additionally, Defendant used biometric timekeeping devices and required workers and individuals to use them in order to eliminate false-positive identifications such as "buddy clocking" and other forms of timekeeping fraud.

47. Defendant subsequently scanned and stored Plaintiff's fingerprint data in its database as a part of the workers' time-clocking process.

48. When Plaintiff began work, Defendant required him to scan his fingerprint before beginning his job functions. Defendant also required him to scan his fingerprint at the end of his workdays.

49. Plaintiff has never been informed in writing that Defendant was capturing, collecting, storing, or using Plaintiff's biometric information.

50. Plaintiff has never been informed of any biometric data retention policy developed by Defendant, nor was he ever informed of whether Defendant would ever permanently delete his biometric information.

51. Plaintiff was never provided with nor ever signed a written release allowing Defendant to collect or store their biometric information.

52. Additionally, Defendant did not obtain consent for any transmission to third parties of Plaintiff's and other workers and individuals' biometrics. To the extent Defendant uses outside vendors to operate its biometrics program in conformance with biometric industry practice, Defendant has also violated BIPA on each occasion it transmits such information to third parties.

53. To this day, Plaintiff is unaware of the status of his biometric information that Defendant obtained. Defendant has not informed Plaintiff whether it still retains his biometric information, and if it does, for how long it intends to retain such information without his consent. Plaintiff's biometric information is economically valuable and such value will increase as the commercialization of biometrics continues to grow.

54. Upon information and belief, Defendant does not have a policy of informing its workers in any way what happens to their biometric information after it is captured, collected, and obtained, whether the information is transmitted to a third party and, if so, which third party, and

what would happen to the information if an individual discontinues working for Defendant, if a facility were to close, or if Defendant were to be acquired, sold, or file for bankruptcy.

55. By failing to comply with BIPA's mandatory notice, release, and policy publication requirements, Defendant has violated workers' substantive rights protected under BIPA and, as a result, Plaintiff and similarly situated individuals continuously have been exposed to substantial and irreversible loss by Defendant's retention of their biometric information without their consent, with such constant and ongoing exposure constituting a severe harm and violation of their rights.

CLASS ALLEGATIONS

56. Plaintiff brings this lawsuit pursuant to 735 ILCS 5/2-801 on behalf of himself and a class of similarly situated individuals, defined as follows (the "Class"):

> All individuals whose biometrics were captured, collected, obtained, stored or used by Defendant within the state of Illinois at any time within the applicable limitations period.

57. Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or amended complaint.

58. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but on information and belief exceeds 100, in which case, individual joinder is impracticable. Defendant has collected, captured, received, or otherwise obtained biometric identifiers or biometric information from over 100 individuals who fall into the definition of the Class. Ultimately, the Class members will be easily identified through Defendant's records.

59. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and Class, and those questions predominate over any questions that may affect individual members, and frame issues for class-wide adjudication. Common

questions for the Class include, but are not necessarily limited to the following:

A. Whether Defendant has a practice of capturing, collecting, storing or using Class members' biometrics;

B. Whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and information when the initial purpose for collecting and obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with Defendant, whichever occurs first;

C. Whether Defendant obtained an executed written release from fingerprinted workers before capturing, collecting, or otherwise obtaining their biometrics;

D. Whether Defendant obtained an executed written release from fingerprinted workers, before capturing, collecting, converting, sharing, storing or using their biometrics;

E. Whether, in order to collect biometrics, Defendant provided a writing disclosing to workers the specific purposes for which the biometrics are being collected, stored and used;

F. Whether, in order to collect biometrics, Defendant provided a writing disclosing to fingerprinted workers the length of time for which the biometrics are being collected, stored and used;

G. Whether Defendant's conduct violates BIPA;

H. Whether Plaintiff and the Class are entitled to damages, and what is the proper measure thereof; and

I. Whether Plaintiff and the Class are entitled to injunctive relief.

60. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interest of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

61. **Appropriateness**: This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economics of time, effort and expense will be fostered and uniformity of decisions will be ensured.

FIRST CAUSE OF ACTION

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

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

63. 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).

64. Defendant fails to comply with these BIPA mandates.

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

66. Plaintiff and the Class are individuals who have their "biometric identifiers" collected by Defendant (in the form of their fingerprints). *See* 740 ILCS § 14/10.

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

68. Defendant failed to publish 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).

69. 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 or 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.

70. On behalf of himself 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 intentional 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

Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

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

72. BIPA requires companies to obtain informed written consent from individuals before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS § 14/15(b) (emphasis added).

73. Defendant fails to comply with these BIPA mandates.

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

75. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected by Defendant (in the form of their fingerprints). *See* 740 ILCS § 14/10.

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

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

78. Defendant did not inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, stored, used and disseminated, nor did Defendant inform Plaintiff and the Class in writing of the specific purpose(s) 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).

79. 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 their biometric identifiers or biometric information as set forth in BIPA. See 740 ILCS § 14/1, *et seq.*

80. On behalf of themselves 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 intentional 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).

THIRD CAUSE OF ACTION

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

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

82. 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).

83. Defendant fails to comply with this BIPA mandate.

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

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

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

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

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

89. On behalf of themselves 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, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional 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, Plaintiff Devonte Grant 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 Devonte Grant as Class Representative, and appointing Law Office of Thomas M. Ryan, P.C. and Law Office of James X. Bormes, P.C. as Class Counsel;

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

C. Awarding statutory damages of $5,000 for each intentional 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 intentional and/or reckless;

E. 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;

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

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

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

Dated: January 4, 2021

Respectfully Submitted,
Devonte Grant, individually and on behalf of all others similarly situated,

By: /s/ Thomas M. Ryan
One of Plaintiff's Attorneys

Thomas M. Ryan
Law Office of Thomas M. Ryan, P.C.
35 E. Wacker Drive, Suite 650
Chicago, IL 60601
312.726.3400
tom@tomryanlaw.com

James X. Bormes
Catherine P. Sons
Law Office of James X. Bormes, P.C.
8 S. Michigan Ave., Suite 2600
Chicago, IL 60603
312.201.0575
bormeslaw@sbcglobal.net
cpsons@bormeslaw.com