☐ YES ☑ NO

EXHIBITS

CASE NO. 22ch 5145

DATE: 5-26-22

CASE TYPE: Class Action

PAGE COUNT: 17

CASE NOTE

_____

_____

_____

Hearing Date: 9/29/2022 10:00 AM
Location: Court Room 2601
Judge: Mitchell, Raymond W.

12-Person Jury

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

NATASHA R. JONES, individually and on behalf of similarly situated individuals,	))))
Plaintiff,	)) Case No. **2022CH05145**
v.	))
MICROSOFT CORPORATION, a Washington corporation,	)))
Defendant.	)))

<u>CLASS ACTION COMPLAINT & JURY DEMAND</u>

Plaintiff, Natasha R. Jones, by and through her undersigned attorneys, brings this Class

Action Complaint against Defendant Microsoft Corporation ("Microsoft" or "Defendant") to seek

redress on her own behalf and on behalf of similarly situated individuals for Defendant's violations

of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* Plaintiff alleges as

follows based on personal knowledge as to her own acts and experiences, and on information and

belief as to all other matters, including an investigation by her attorneys.

INTRODUCTION

1.   While many employers use straightforward methods to allow their employees to

clock-in and clock-out of work, such as ID badges or conventional punch clocks, some employers

require that employees—as a condition of employment—have their fingerprints scanned by a

device or application.

2.   Unlike ID badges or pass codes, which can be easily changed or replaced if stolen

or compromised, a fingerprint is a unique, permanent biometric identifier associated with each

employee. Employers' use of this technology exposes their 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, employees have no practical means by which to prevent identity theft, unauthorized tracking, or other unlawful or improper use of this highly personal and private information.

3. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA") specifically to regulate companies that collect, obtain, store, use, and/or disseminate Illinois citizens' biometrics, such as fingerprints.

4. Defendant is an entity subject to BIPA, as it stores myriad types of data, including biometrics, on behalf of a wide range of employers spanning virtually every industry sector. Specifically, Defendant offers cloud storage services for businesses that collect biometric identifiers and biometric information. For example, some of Defendant's customers are commercial businesses that require their employees to provide their biometrics, such as fingerprints, to clock in and out of their shifts at work. In such a scenario, Defendant obtains and stores data and information that is generated as a result of the capture, collection, and processing of biometric identifiers. This information is considered "biometric information" subject to regulation under BIPA.

5. Despite obtaining, storing, and possessing Illinois residents' biometric information—including Plaintiff's biometrics—on behalf of its customers, Defendant has failed to comply with BIPA in multiple ways.

6. Accordingly, Plaintiff brings this action for damages and other relief as a result of Defendant's conduct in violating her biometric privacy rights under BIPA. On behalf of herself and the proposed Class defined below, Plaintiff seeks an injunction requiring Defendant to comply with BIPA, as well as an award of statutory damages to the Class members in an amount to be

2

determined at trial, together with costs and reasonable attorneys' fees.

PARTIES

7.   Plaintiff, Natasha R. Jones, is a natural person and at all relevant times has been a resident of Illinois.

8.   Defendant, Microsoft Corporation, is a for-profit corporation organized under the laws of Washington and headquartered in Redmond, Washington. Defendant maintains a registered agent in Illinois and is licensed to conduct business in Illinois, and does in fact conduct substantial business throughout Illinois, including in Cook County, Illinois.

JURISDICTION AND VENUE

9.   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 knowingly doing business within this State such that it has sufficient minimum contacts with Illinois and has purposely availed itself of Illinois markets to make it reasonable for this Court to exercise jurisdiction over Defendant, and because Plaintiff's claims arise out of or relate to Defendant's conduct in Illinois, as Defendant transacts with and provides cloud-based storage for employers that captured, collected, stored, and used Plaintiff's and the other putative Class members' biometric identifiers and/or biometric information in this State.

10.   Venue is proper in Cook County pursuant to 735 ILCS 5/2-101, because Defendant is foreign corporation doing business in Cook County and it thus resides there under § 2-102.

THE BIOMETRIC INFORMATION PRIVACY ACT

11.   "Biometrics" refers to a "biology-based set[s] of measurements." *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017). Specifically, "biometrics" are "a set of measurements of a specified physical component (eye, finger, voice, hand, face)." *Id.* at 1296.

3

12.   BIPA was enacted in 2008 in order to safeguard individuals' biometrics as the result of the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA is codified as Act 14 in Chapter 740 of the Illinois Compiled Statutes.

13.   As set forth in BIPA, biologically unique identifiers, such as a person's unique fingerprint, implicate special concerns because they cannot be changed:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. 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.

740 ILCS 14/5(c).

14.   Due to the need for enhanced protection of biometrics, BIPA imposes various requirements on private entities with respect to individuals' biometrics.

15.   Among other things, BIPA seeks to regulate "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g). BIPA thus applies to entities that interact with two forms of Biometric Data: biometric "identifiers" and biometric "information." 740 ILCS 14/15(a)–(e).

16.   BIPA defines a "biometric identifier" as any personal feature that is unique to an individual, including fingerprints, voiceprints, palm scans and facial geometry. "Biometric identifiers" are physiological, as opposed to behavioral, characteristics. BIPA's text provides a non-exclusive list of protected "biometric identifiers," including "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

17.   "Biometric information" is defined by BIPA as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to

4

identify an individual." *Id.* This definition helps ensure that information based on a biometric identifier that can be used to identify a person is covered by BIPA. Collectively, biometric identifiers and biometric information are known as "biometrics."

18.   In Section 15 of BIPA, there is a list of four distinct categories of activities that may subject private entities to liability:

     a. possessing biometrics without making publicly available a written biometric retention and destruction policy, 740 ILCS 14/15(a);

     b. collecting biometrics without informed written consent, 740 ILCS 14/15(b);

     c. profiting from biometrics, 740 ILCS 14/15(c); and

     d. disclosing or disseminating biometrics without consent, 740 ILCS 14/15(d).

19.   Compliance with BIPA is straightforward and may be accomplished through a single, signed sheet of paper.

FACTUAL BACKGROUND

Defendant's Azure Platform

20.   Defendant is the provider of the Azure cloud computing service, which hosts and manages applications and services through Microsoft-managed data centers. Importantly, Azure is also a cloud storage platform for biometric timekeeping providers.

21.   Cloud computing services, such as Azure, allow users to store and access data through the internet rather than storing the data locally. More specifically, cloud technology uses virtual servers to store information rather than maintaining storage on an on-site device. These virtual servers connect to data centers where the information is physically stored.

22.   Defendant's Azure data centers are located throughout the country, including in Illinois. Specifically, Defendant operates a 700,000 square-foot data center in Northlake, Illinois,

and has recently begun constructing data centers in Elk Grove Village, Illinois and Hoffman Estates, Illinois. Importantly, Defendant's Azure North Central US region has its data center located in Illinois.

23.   Defendant offers Microsoft Azure as a "Platform as a Service" product and includes its Azure SQL Database in such service. Azure can be used to host software and other products while also storing sensitive information.

Azure's Integration with Biometric Timeclocks

24.   Biometric timekeeping services work by extracting biometric information from individuals, such as handprints, fingerprints, or portions thereof, and subsequently using the same for authentication and timekeeping purposes. The systems include the dissemination of biometrics to third-parties, such as data storage vendors and payroll services.

25.   One prominent biometric timekeeping provider is Paychex, Inc. ("Paychex"). Paychex provides biometric timekeeping services to employers throughout the state of Illinois. Importantly, Paychex's entire suite of apps, including Paychex Flex Time, are cloud-based apps supported by, and stored on, Defendant's Azure cloud-computing service and at Defendant's data centers.

26.   Paychex is the second largest consumer of Microsoft Azure's public cloud database. Paychex organizes each employer into its own database and now stores over 40,000 of its employers' databases on Azure.

27.   Because it is hosted on Defendant's Azure cloud technology, Paychex Flex Time relies on Defendant's data centers to store the information Paychex Flex Time collects.

28.   The Paychex Flex Time application handles clocking-in and clocking-out and is hosted on Microsoft Azure. Paychex Flex Time processes three million timeclock punches each

day and sends such information to its software hosted by Microsoft Azure.

29.   Numerous employers throughout the state of Illinois use Paychex's biometric timekeeping services to track their employees' time. Paychex has collected and stored around 80,000 employees' biometrics in Illinois while utilizing Defendant's Azure technology.

30.   When employers that use Paychex Flex Time hire new employees, they scan the new employees' fingerprints to enroll them in an employee database hosted by Defendant on Azure.

31.   Employees are then required to use their biometrics to clock-in and clock-out of work to record their time. Such information is transferred and stored on Defendant's Azure service.

32.   When employees' biometrics are uploaded into Paychex Flex Time, Defendant collects, obtains, and stores the employees' fingerprint data to be used as a template with which to compare future fingerprint scans in order to verify the users' identity.

33.   Through the integration of Paychex's Flex Time application with the Azure platform, Defendant collects, obtains, and stores employees' biometrics each time the employees clock-in or clock-out of work.

34.   Despite collecting and storing biometrics with Azure, Defendant fails to comply with BIPA's statutory requirements, thereby depriving employees of their statutory rights.

35.   Although Defendant collects and stores biometrics of its clients' employees, including Plaintiff's and the other Class members' biometrics, Defendant failed to obtain proper written consent as required by BIPA to collect such biometrics.

36.   Further, Defendant failed to make publicly available a written policy as to Defendant's retention and deletion practices regarding the biometrics in its possession.

37.   Defendant also unlawfully profited from the biometrics it obtained from its clients'

7

employees, including Plaintiff and the other Class members, as Defendant was paid by its clients for access to Defendant's Azure cloud computing services.

FACTS SPECIFIC TO PLAINTIFF

38. Plaintiff began working for Chicago Marriott Suites in or around October 2015 and continued working there for approximately six years.

39. As a condition of her employment, Plaintiff was required to scan and register her fingerprint for timekeeping purposes.

40. Plaintiff's employer registered her fingerprint through Paychex, the employer's biometric timekeeping service provider.

41. Paychex utilizes Defendant's Azure platform to provide such biometric timekeeping services.

42. Accordingly, Defendant obtained and stored Plaintiff's and other Class members' biometrics on its Azure database.

43. Plaintiff was required to provide biometric scans each time she needed to clock in and clock out of a shift at work.

44. However, Defendant collected, obtained, and stored electronic information derived from the scanning of Plaintiff's biometric identifiers without first informing Plaintiff in writing that Plaintiff's biometrics were being collected, stored, used, or disseminated, or publishing any policy addressing its biometric retention and destruction schedules, as required by BIPA.

45. Nor did Defendant seek, and Plaintiff never provided to Defendant, any written consent.

46. By failing to comply with BIPA, Defendant has violated Plaintiff's substantive state law rights to biometric privacy.

CLASS ALLEGATIONS

47.   Plaintiff brings this action both individually on her own behalf and, pursuant to 735

ILCS § 5/2-801, as representative on behalf of a Class defined as follows:

> Class: All individuals whose biometrics were captured, collected, stored, used, transmitted, or disseminated by an employer using timekeeping software hosted on Defendant's Azure service within the state of Illinois at any time within the applicable limitations period.

48.   Excluded from the Class are any members of the judiciary assigned to preside over

this matter; any officer or director of Defendant; and any immediate family member of such

individuals.

49.   Upon information and belief, there are hundreds if not thousands of members of the

Class, making the members of the Class so numerous that joinder of all members is impracticable.

Although the exact number of members of the Class is currently unknown to Plaintiff, the members

can be easily identified through Defendant's records and the personnel records of Defendant's

employer-customers.

50.   Plaintiff's claims are typical of the claims of the members of the Class that Plaintiff

seeks to represent, because the factual and legal bases of Defendant's liability to Plaintiff and the

other Class members are the same, and because Defendant's conduct has resulted in similar harms

to Plaintiff and to the Class. As alleged herein, Plaintiff and the Class have all been aggrieved as

a result of Defendant's BIPA violations.

51.   There are many questions of law and fact common to the claims of Plaintiff and the

Class, and those questions predominate over any questions that may affect individual members.

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

  a. Whether Defendant's conduct with respect to the Azure platform is subject to BIPA;

  b. Whether Defendant made available to the public a written policy that establishes a

9

retention schedule and guidelines for destroying biometrics;

c. Whether Defendant obtained a written release from the Class members before capturing, collecting, storing, or otherwise obtaining their biometrics;

d. Whether Defendant provided a written disclosure that explains the specific purposes, and the length of time, for which biometrics were being collected, stored, and used before receiving such biometrics;

e. Whether Defendant profited from the Class's biometrics;

f. Whether Defendant disclosed or otherwise disseminated the Class's biometrics without the requisite consent;

g. Whether Defendant's conduct violates BIPA;

h. Whether Defendant's violations of BIPA are willful or reckless; and

i. Whether Plaintiff and the Class are entitled to damages and injunctive relief.

52. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions in that it conserves the resources of the courts and the litigants and promotes consistency of adjudication.

53. Plaintiff will adequately represent and protect the interests of the members of the Class. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the members of the Class.

54. Defendant has acted and failed to act on grounds generally applicable to Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure

10

compatible standards of conduct toward the members of the Class and making injunctive or

corresponding declaratory relief appropriate for the Class as a whole.

COUNT I
Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(a)
(On behalf of Plaintiff and the Class)

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

56.   Defendant is a private entity subject to BIPA. 740 ILCS 14/10.

57.   As discussed above, Plaintiff and the other Class members have had their

"biometric identifiers," namely their fingerprints and/or data derived therefrom, *i.e.* "biometric

information," collected and stored, and thus possessed, by Defendant as a result of interacting with

timekeeping services hosted on Defendant's Azure platform.

58.   Section 15(a) of BIPA requires any entity in possession of biometric identifiers or

biometric information to "develop 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 3 years of the individual's last interaction with the private entity, whichever

occurs first." 740 ILCS 14/15(a).

59.   Though Defendant has come into possession of Plaintiff's and other Class

members' biometric identifiers, it has failed to make publicly available any policy addressing its

biometric retention and destruction practices.

60.   As a result, Defendant has violated Section 15(a) of BIPA.

61.   Defendant knew, or was reckless in not knowing, that its Azure platform which

numerous Illinois residents interacted with, would be subject to Section 15(a) of BIPA, a statutory

provision passed in 2008, yet failed to comply with the statute.

62.   BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)–(2).

63.   Defendant's violations of Section 15(a) of BIPA, a statutory provision that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with Section 15(a) of BIPA

64.   Accordingly, with respect to Count I, Plaintiff, individually and on behalf of the proposed Class, prays for the relief set forth below.

COUNT II
Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(b)
(On behalf of Plaintiff and the Class)

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

66.   Defendant is a private entity subject to BIPA. 740 ILCS 14/10.

67.   As discussed above, Plaintiff and the other Class members have had their "biometric identifiers," namely their fingerprints and/or data derived therefrom, *i.e.* "biometric information," collected, captured, and stored by Defendant on its Azure platform.

68.   BIPA requires a private entity, such as Defendant, to obtain informed written consent from individuals before acquiring their biometric identifiers or biometric information. Specifically, under BIPA it is unlawful to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or 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 for which a biometric identifier or biometric information is being captured, collected, stored, and used; and (3) receives a written release executed by the subject of the

12

biometric identifier or biometric information . . . ." 740 ILCS 14/15(b).

69.   In each instance when Plaintiff and the other Class members interacted with their employers' biometric timekeeping systems, Defendant captured, collected, or otherwise obtained Plaintiff's and the other Class members' biometrics without their written consent and without complying with and, thus, in violation of BIPA.

70.   Defendant's practices with respect to capturing, collecting, storing, and using biometrics fails to comply with applicable BIPA requirements:

a.   Defendant failed to inform Plaintiff and the members of the Class in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);

b.   Defendant failed to inform Plaintiff and the Class in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

c.   Defendant failed to inform Plaintiff and the Class in writing the specific length of term their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2); and

d.   Defendant failed to obtain a written release, as required by 740 ILCS 14/15(b)(3).

71.   As a result, Defendant has violated Section 15(b) of BIPA.

72.   Defendant knew, or was reckless in not knowing, that its Azure platform which numerous Illinois residents interacted with, would be subject to Section 15(b) of BIPA, a statutory provision passed in 2008, yet failed to comply with the statute.

73.   BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740

13

74.   Defendant's violations of Section 15(b) of BIPA, a statutory provision that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with Section 15(b) of BIPA.

75.   Accordingly, with respect to Count II, Plaintiff, individually and on behalf of the proposed Class, prays for the relief set forth below.

COUNT III
Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(c)
(On behalf of Plaintiff and the Class)

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

77.   Defendant is a private entity subject to BIPA. 740 ILCS 14/10.

78.   As discussed above, Plaintiff and the other Class members have had their "biometric identifiers," namely their fingerprints and/or data derived therefrom, *i.e.* "biometric information," collected, captured, and stored by Defendant on its Azure platform.

79.   Section 15(c) of BIPA prohibits any private entity in possession of biometrics, such as Defendant, from selling, leasing, trading, or otherwise profiting from such biometrics. 740 ILCS 14/15(d).

80.   As alleged herein, Defendant profited from the biometrics it obtained from its clients' employees, including Plaintiff and the other Class members, as Defendant was paid by its clients for access to Defendant's Azure platform. On information and belief, Defendant charges its clients based on the amount of data it stores on their behalf, such that Defendant's profits are dependent at least in part on the amount of biometric data it stores. Thus, Defendant profited directly from Plaintiff's and the other Class members' biometrics.

81.   Accordingly, Defendant has violated Section 15(c) of BIPA.

14

82.   Defendant knew, or was reckless in not knowing, that its Azure platform which numerous Illinois residents interacted with, would be subject to Section 15(c) of BIPA, a statutory provision passed in 2008, yet failed to comply with the statute.

83.   BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)–(2).

84.   Defendant's violations of Section 15(c) of BIPA, a statutory provision that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with Section 15(c) of BIPA.

85.   Accordingly, with respect to Count III, Plaintiff, individually and on behalf of the proposed Class, prays for the relief set forth below.

<div align="center">

COUNT IV
Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(d)
(On behalf of Plaintiff and the Class)

</div>

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

87.   Defendant is a private entity subject to BIPA. 740 ILCS 14/10.

88.   As discussed above, Plaintiff and the other Class members have had their "biometric identifiers," namely their fingerprints and/or data derived therefrom, *i.e.* "biometric information," collected, captured, and stored by Defendant on its Azure platform.

89.   Section 15(d) of BIPA prohibits any private entity in possession of biometrics, such as Defendant, from disclosing, redisclosing, or otherwise disseminating an individual's biometric identifiers or biometric information without that individual's consent. 740 ILCS 14/15(d).

90.   As alleged herein, after Plaintiff's and other Class members' biometric identifiers were obtained by Defendant through its clients' platforms, Defendant disclosed or otherwise

<div align="center">15</div>

disseminated their biometrics.

91.　Defendant never obtained Plaintiff's or other Class members' consent to disclose or disseminate their biometrics.

92.　Accordingly, Defendant has violated Section 15(d) of BIPA.

93.　Defendant knew, or was reckless in not knowing, that its Azure platform which numerous Illinois residents interacted with, would be subject to Section 15(d) of BIPA, a statutory provision passed in 2008, yet failed to comply with the statute.

94.　BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)–(2).

95.　Defendant's violations of Section 15(d) of BIPA, a statutory provision that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with Section 15(d) of BIPA.

96.　Accordingly, with respect to Count IV, Plaintiff, individually and on behalf of the proposed Class, prays for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that this Court enter an Order:

a.　Certifying the Class as defined above, appointing Plaintiff as class representative and the undersigned counsel as class counsel;

b.　Declaring that Defendant's actions, as set forth herein, violate BIPA;

c.　Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA;

16

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of BIPA, pursuant to 740 ILCS 14/20(2);

e. Awarding statutory damages of $1,000 for each negligent violation of BIPA, pursuant to 740 ILCS 14/20(1);

f. Awarding reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);

g. Awarding pre- and post-judgment interest, as allowable by law; and

h. Awarding such further and other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Dated: May 26, 2022

Respectfully submitted,

NATASHA R. JONES, individually and on behalf of similarly situated individuals

By: /s/ *Steven Beckham*
One of Plaintiff's Attorneys

Myles McGuire
Paul T. Geske
Steven R. Beckham
MCGUIRE LAW, P.C. (Firm ID: 56618)
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
Fax: (312) 275-7895
mmcguire@mcgpc.com
pgeske@mcgpc.com
sbeckham@mcgpc.com

Attorneys for Plaintiff and the putative Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Microsoft Unlawfully Stored Illinois Workers' Fingerprints on Azure Databases, Class Action Alleges](#)