Return Date: No return date scheduled
Hearing Date: No hearing scheduled
Courtroom Number: No hearing scheduled
Location: No hearing scheduled

FILED
12/14/2020 1:26 PM
IRIS Y. MARTINEZ
CIRCUIT CLERK
COOK COUNTY, IL
2019CH14082

11481231

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

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

JOE FISHER, individually, and on behalf of all others similarly situated,	)	
Plaintiff,	)	
v.	)	**Case No. 2019-CH-14082**
HP PROPERTY MANAGEMENT LLC and MARCON INTERNATIONAL, INC. d/b/a KEYPER SYSTEMS,	)	
Defendants.	)	

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiff Joe Fisher ("Plaintiff" or "Fisher"), individually and on behalf of all others similarly situated (the "Class"), by and through his attorneys, brings the following Second Amended Class Action Complaint pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against HP Property Management LLC and Marcon International, Inc. d/b/a KEYper Systems (collectively, "Defendants"), their subsidiaries and affiliates, to redress and curtail Defendants' unlawful collection, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric data. Plaintiff alleges as follows upon personal knowledge as to himself, his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. Defendant HP Property Management LLC ("HP Property") is a company that manages residential rental properties on the south side of Chicago.

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

2. While many property management companies use conventional methods for managing keys to rental properties, individuals authorized to access keys to rental properties by HP Property and its affiliated companies are required to have their fingerprints scanned by a biometric device using hardware and software licensed by Marcon International, Inc. d/b/a KEYper Systems.

3. Marcon International, Inc. d/b/a KEYper Systems ("KEYper Systems") is a security company that provides key storage and key management systems, padlock management for "lock out" or "tag out" procedures, and asset control of equipment.

4. KEYper Systems prides itself on providing the most robust and secure key management equipment to various industries including automotive services, government agencies, and property management.

5. With this focus on security, KEYper Systems products "come complete with visual and audible alarms, built-in biometric fingerprint or prox reader, digital security camera and provide comprehensive reporting and analytics along with multi-system networking." *KEYper Systems*, Lenel United Technologies, *available at* https://www.lenel.com/solutions/open-integration/oaap/partners-products-search/keyper-systems.

6. KEYper Systems boasts that this multi-system network ensures efficiency due to the fact that it is fully automated and "[e]very activity is recorded in the system's memory." *The Importance of Electronic Key Management for Fleet Operators*, KEYper Systems (July 26, 2018) *available at* https://www.keypersystems.com/benefits-of-hotel-key-management/.

7. When HP Property and its affiliates authorize property managers, leasing team members, construction team members, marketing team members, and other workers, including Plaintiff, to use the KEYper Systems device, users are first enrolled in KEYper Systems' biometric

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

database(s) using a scan of their fingerprint and entering their name, email, and password information into the system. HP Property then uses the biometric data to grant users access to property keys.

8. Upon information and belief, Plaintiff's and other users' biometric data is shared and maintained by and between Defendants, which use the KEYper Systems device to manage the security of keys to rental properties managed by HP Property.

9. KEYper Systems has ongoing access to the biometric data stored in its biometric database(s) after an individual is enrolled to use the device. According to KEYper Systems' terms and conditions governing the provision of hardware, software, and services to its customers, customers, such as HP Property, grant KEYper Systems "the right to host, use, process, display and transmit Customer Content," which includes the personal data of users. *Terms and Conditions*, KEYper Systems *available at* https://www.keypersystems.com/terms-and-conditions/ (accessed Apr. 23, 2020). KEYper Systems uses or processes user personal data of for the purpose of providing its services, which include "the back-up storage of Customer Content and User Data, for which KEYper receives, stores, accesses or otherwise processes Personal Data." *Id.* KEYper Systems defines Personal Data as "any information relating to an identified or identifiable natural person." *Id.* With regard to information security, KEYper Systems represents that it "may rely upon the security processes and measures utilized by KEYper's cloud infrastructure providers." *Id.*

10. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as HP Property – 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.

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

11. Unlike ID badges or pass codes – which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with each individual. Defendants' use of this technology exposes users 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, Facebook/Cambridge Analytica, and Suprema data breaches or misuses – individuals have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

12. 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.

13. 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 handprints, 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=.b3c70259f138.

14. 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),

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

available at http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

15. 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 in 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.

16. In the United States, law enforcement, including the Federal Bureau of Investigation and Immigration and Customs Enforcement, have attempted to turn states' Department of Motor Vehicles databases into biometric data goldmines, using facial recognition technology to scan the faces of thousands of citizens, all without their notice or consent. Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, The Washington Post (July 7, 2019), *available at* https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/?noredirect=on&utm_term=.da9afb2472a9.

17. 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-facial-recognition-requests-14081967.php.

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

18. 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.

19. Notwithstanding the clear and unequivocal requirements of the law, each Defendant disregarded Plaintiff's and other similarly-situated individuals' statutorily protected privacy rights and unlawfully collect, store, disclose, and use individuals' biometric data in violation of BIPA. Specifically, each Defendant has violated and continues to violate BIPA because it did not and continues not to:

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

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

c. Receive a written release from Plaintiff and others similarly situated to collect, store, disclose, 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.

20. Plaintiff and other similarly-situated individuals are aggrieved because they were not: (1) informed in writing of the purposes and length of time for which their fingerprints were being collected, stored, 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.

21. Defendant HP Property has improperly disclosed Plaintiff's and other similarly-situated individuals' fingerprint data to KEYper Systems and, upon information and belief, to other

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

currently unknown third parties, including but not limited to third parties that host biometric data in their data centers or cloud infrastructure.

22. Upon information and belief, each Defendant lacks a retention schedule 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.

23. Plaintiff and other similarly-situated individuals have a proprietary right to control their biometric information. In failing to comply with the requirements of BIPA, each Defendant has intentionally interfered with each individual's right of possession and control over his or her valuable, unique, and permanent biometric data.

24. Defendants are directly liable for, and had actual knowledge of, the BIPA violations alleged herein.

25. 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

26. Plaintiff Joe Fisher is a natural person and a citizen of the State of Illinois.

27. Defendant HP Property Management LLC is a limited liability company organized and existing under the laws of the State of Illinois, with its principal place of business located at 1421 East 53rd Street, Suite 100, Chicago, Illinois 60615. HP Property Management LLC is registered with the Illinois Secretary of State and conducts business in the State of Illinois, including Cook County.

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

28. Defendant Marcon International, Inc. d/b/a KEYper Systems is a corporation organized and existing under the laws of the State of North Carolina, with its principal place of business located at 5679 Harrisburg Industrial Park Drive, Harrisburg, North Carolina 28075. Marcon International, Inc. conducts business in the State of Illinois, including Cook County.

JURISDICTION AND VENUE

29. This Court has jurisdiction over Defendants pursuant to 735 ILCS § 5/2-209 because Defendants transact business within Illinois and committed the statutory violations alleged herein in Illinois.

30. Venue is proper in Cook County because Defendants transact business in Cook County and committed the statutory violations alleged herein in Cook County.

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act.

31. 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.

32. 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. 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

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

protections for 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.

33. 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.

34. 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.

35. 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 or 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).

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

36. 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*.

37. 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 such disclosures. *See* 740 ILCS § 14/15(d)(1).

38. 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).

39. 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 a heightened risk for identity theft and left without any recourse.

40. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics. BIPA also protects individuals' rights to know the precise

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

nature for which their biometrics are used and how they are being stored and ultimately destroyed, allowing individuals to make a truly informed choice. 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 disclose biometrics and creates a private right of action for lack of statutory compliance.

41. 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.

42. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had experimented with using individuals' biometric data stopped doing so.

43. However, each Defendant failed to take note of the shift in Illinois law governing the collection, use, storage, and disclosure of biometric data. As a result, each Defendant continues to collect, store, use and disclose individuals' biometric data in violation of BIPA.

44. Specifically, when HP Property and its affiliated companies grant workers access to the keys to rental properties, they require authorized users to scan their fingerprint to enroll them in KEYper Systems' biometric database(s).

45. HP Property uses a KEYper Systems biometric device and software supplied by KEYper Systems that requires authorized users to use their fingerprint as a means of authentication. Authorized users are required to scan their fingerprints to access keys to rental properties.

46. When authorized users enroll their fingerprint data into the KEYper Systems biometric database(s), HP Property captures, collects, and stores the users' fingerprint data to be

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

used as a template with which to compare future fingerprint scans in order to verify the users' identity.

47. HP Property again collects authorized users' fingerprint data upon each subsequent fingerprint scan.

48. HP Property discloses authorized users' fingerprint data to at least one out-of-state third-party vendor, KEYper Systems, which received, stored, accessed or otherwise processed the biometric data the purpose of providing its services, including the back-up storage of data, and likely others who host the biometric data in their data centers.

49. Upon information and belief, KEYper Systems discloses HP Property authorized users' fingerprint data to other, currently unknown, third parties, which host the biometric data in their data centers or cloud infrastructure.

50. HP Property failed and continues to fail to inform authorized users that it discloses or disclosed their sensitive biometric data to at least one out-of-state third-party vendor, KEYper Systems, and likely others; fails to inform users that it discloses or disclosed their biometric data to currently-unknown third parties, which host the biometric data in their data centers; fails to inform users of the purposes and duration for which it collects their biometric data; and fails to obtain written releases from users before collecting their fingerprints, as required by BIPA.

51. KEYper Systems failed and continues to fail to inform authorized users of its device that it discloses their sensitive biometric data to other, currently unknown, third parties, which host the biometric data in their data centers or cloud infrastructure; fails to inform users of the purposes and duration for which it collects their biometric data; and fails to obtain written releases from users before collecting their fingerprints, as required by BIPA.

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

52. At no time did either Defendant secure written releases from authorized users before collecting their biometric information.

53. Furthermore, each Defendant fails to publish a written, publicly available policy identifying their retention schedules and guidelines for permanently destroying authorized users' biometric data when the initial purpose for collecting or obtaining their biometric data is no longer relevant, as required by BIPA.

54. The Pay by Touch bankruptcy that catalyzed the passage of BIPA, as well as the recent data breaches, highlight why such conduct – where individuals are aware that they are providing a fingerprint, but not aware of 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 their fingerprints, who exactly is collecting their biometric data, where it will be transmitted, for what purposes, and for how long. Each Defendant disregards these obligations and the statutory rights of authorized users and instead unlawfully collects, stores, uses and discloses their biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

55. Each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and has 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.

56. No Defendant told Plaintiff or others similarly situated what might happen to their biometric data if and when either of the Defendants merge with another company – or worse, if

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

and when either of the Defendants' business folds, or when the other third parties that have received users' biometric data businesses fold.

57. Since Defendants neither publish a BIPA-mandated data-retention policy nor disclose all of the purposes for their collection and use of biometric data, users have no idea the extent to which each Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and others similarly situated are not told the extent to whom each Defendant currently discloses their biometric data, or what might happen to their biometric data in the event of a merger or a bankruptcy.

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

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

III. Plaintiff Joe Fisher's Experience.

60. Plaintiff Joe Fisher worked for HP Property as a portfolio manager from approximately July 2017 until September 2019.

61. On or about June 2018, HP Property installed a KEYper Systems biometric device at its office at 5316 South Dorchester Avenue in Chicago, Illinois, and Plaintiff and all other authorized individuals were required to enroll in KEYper Systems' biometric database(s) by scanning their fingerprints and entering their names, emails and passwords. HP Property used Plaintiff's and other individuals' fingerprint data as an authentication method to manage access to keys to rental properties.

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

62. When HP Property moved to a new office at 1421 East 53rd Street in Chicago, Illinois, the KEYper Systems device was also moved to the new location and Plaintiff was re-enrolled in the system a second time via a fingerprint scan.

63. Upon information and belief, each Defendant has collected, stored, used, and/or disclosed Plaintiff's and other similarly-situated individuals' fingerprint data.

64. Plaintiff was required to scan his fingerprint each time he accessed a key to a rental property.

65. Plaintiff was never informed, prior to the collection of his biometric identifiers and/or biometric information, of the specific limited purposes or length of time for which any Defendant collected, stored, used, and/or disclosed his biometric data.

66. Plaintiff has no knowledge of any biometric data retention policy developed by any Defendant and made available to the public, nor has he ever been informed of whether any Defendant will ever permanently delete his biometric data.

67. Plaintiff has never been provided with nor ever signed a written release allowing any Defendant to collect, store, use or disclose his biometric data.

68. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendants' multiple violations of BIPA alleged herein.

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

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

70. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act").

71. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, he seeks statutory damages under BIPA as compensation for the injuries caused by Defendants. *Rosenbach*, 2019 IL 123186, ¶ 40. Nonetheless, Plaintiff is aggrieved because he suffered an injury-in-fact based on Defendants' violations of his legal rights. Defendants have intentionally interfered with Plaintiff's right to possess and control his own sensitive biometric data. Additionally, Plaintiff suffered an invasion of a legally protected interest when Defendants secured his personal and private biometric data at a time when they had no right to do so, a gross invasion of his right to privacy. BIPA protects individuals like Fisher 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.

72. Plaintiff's biometric information is economically valuable, and such value will increase as the commercialization of biometrics continues to grow.

73. Plaintiff also suffered an informational injury because each Defendant has failed to provide him with information to which he was entitled by statute. Through BIPA, the Illinois legislature has created a right: an individual's right to receive certain information prior to a company securing his or her highly personal, private and proprietary biometric data; and an injury – not receiving this extremely critical information.

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

74. Plaintiff also suffered an injury in fact to the extent each Defendant has improperly disclosed his biometric identifiers and/or biometric information to third parties that hosted the biometric data in their data centers or cloud infrastructure, in violation of BIPA.

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

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

CLASS ALLEGATIONS

77. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS § 5/2-801, Plaintiff brings claims on his 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.

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

78. 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(s) 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.

79. Plaintiff seeks class certification under the Illinois Code of Civil Procedure, 735 ILCS § 5/2-801, for the following class of similarly-situated individuals under BIPA:

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

80. 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. Plaintiff's claims are typical of the claims of the class; and,

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

Numerosity

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

Commonality

82. 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

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

harmed by each Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether each Defendant collected, captured, maintained, stored, or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

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

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

D. Whether each Defendant disclosed or redisclosed Plaintiff's and the Class's biometric identifiers or biometric information;

E. Whether any Defendant has sold, leased, traded, or otherwise profited from Plaintiff's and the Class'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 each Defendant used Plaintiff's and the Class's fingerprints to identify them;

I. Whether any Defendant's violations of BIPA have raised a material risk that Plaintiff's and the putative Class' 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 intentionally or recklessly.

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

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

Adequacy

84. 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 that are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

85. The claims asserted by Plaintiff are typical of the class members he seeks to represent. Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

86. 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

87. 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

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

would make it difficult for individual class members to vindicate their claims.

88. 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 each Defendant and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

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

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

90. 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).

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

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

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

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

94. 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.

95. Each 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).

96. 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 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.

97. 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 each 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

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

99. BIPA requires companies to obtain informed written consent from individuals before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

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).

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

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

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

103. 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.

104. Each Defendant systematically and automatically collected, captured, received through trade, or otherwise obtained 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).

105. No Defendant informed Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, captured, received through trade, or otherwise obtained, nor did any 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, and used as required by 740 ILCS § 14/15(b)(1)-(2).

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

106. By collecting, capturing, receiving through trade, or otherwise obtaining 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*.

107. 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 each 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

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

109. 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).

110. Each Defendant failed to comply with this BIPA mandate.

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

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

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

113. 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.

114. Each 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).

115. By disclosing, redisclosing, or otherwise disseminating 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.*

116. 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 each Defendant to comply with BIPA's requirements for the collection, storage, use and disclosure 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 Joe Fisher 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 Joe Fisher as Class Representative, and appointing Stephan Zouras, LLP, as Class Counsel;

B. Declaring that each 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

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

damages of $1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS § 14/20(1);

D. Declaring that each 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 each Defendant to collect, store, use and disclose 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.

Date: December 14, 2020

Respectfully Submitted,

/s/ Ryan F. Stephan

Ryan F. Stephan
Teresa M. Becvar
Stephan Zouras, LLP
100 N. Riverside Plaza, Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com
tbecvar@stephanzouras.com
Firm ID: 43734

ATTORNEYS FOR PLAINTIFF

FILED DATE: 12/14/2020 1:26 PM 2019CH14082

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on December 14, 2020, I filed the attached with the Clerk of the Court using the Court's electronic filing system, which will send such filing to all attorneys of record.

Debra R. Bernard
PERKINS COIE LLP
131 South Dearborn Street, Suite
1700 Chicago, IL 60603-5559
dbernard@perkinscoie.com

Jamie L. Filipovic
Collin D. Woodward
O'Hagan Meyer LLC
One E. Wacker Dr., Ste. 3400
Chicago, IL 60601
jfilipovic@ohaganmeyer.com
cwoodward@ohaganmeyer.com

/s/ Ryan F. Stephan