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

RAY MCGEE, individually and on behalf of a class of similarly situated individuals, *Plaintiff*, v. LSC COMMUNICATIONS, INC., a Delaware corporation and FAIRRINGTON, LLC, a Delaware limited liability company, *Defendants*.	)	Case No. 17-CH-12818 Hon. David B. Atkins

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Ray McGee ("Plaintiff"), individually and on behalf of other similarly situated individuals, brings this First Amended Class Action Complaint against Defendants LSC Communications, Inc. and Fairrington, LLC (together, "Defendants"), to stop Defendants' unlawful collection, use, and storage of individuals' biometric identifiers and/or biometric information in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. (the "BIPA"), and to obtain redress for all persons injured by their conduct. Plaintiff alleges as follows based on personal knowledge as to his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

INTRODUCTION

1. This case concerns the misuse of individuals' biometric identifiers and/or biometric information by a mailing logistics enterprise which is capturing, converting, transferring, storing and using their workers' biometric information without lawful consent. Defendants do this through the use of biometric scanning devices and associated software technology which capture

a person's fingerprint information derived from their fingerprints to authenticate the identity of such persons in the future.

2. New technology has allowed consumers to pay their bills, secure financial accounts, and purchase physical goods, all with their biometric information, which is often a fingerprint. Unfortunately, along with the increased utility of biometric technology, so too has come grave privacy risks associated with the dissemination and unregulated collection of biometric information. Indeed, the permanent and irreplaceable nature of one's biometrics makes the illegal collection of the same a significant public problem with far-reaching consequences, including irreversible identify theft and potential financial ruin.

3. So substantial is the risk from the wide collection of biometric information by private companies that numerous state legislatures, including Alaska, Connecticut, Montana, Michigan, Texas, New Hampshire, and Washington, have introduced legislation to regulate the collection and use of such sensitive information in an effort to stem the unique problems created by the irreplaceable nature and unique identifying characteristics of biometrics.

4. The Illinois Legislature was the first to pass such legislation into law. In 2007, after a company specializing in the collection of biometric information filed for bankruptcy protection, effectively putting consumers' biometrics up for sale to the highest bidder, the Illinois Legislature knew that the liquidation proceedings created a serious risk that millions of fingerprint records would be sold as an asset or otherwise distributed without the consent, or even knowledge, of the persons to whom such fingerprints belonged.

5. Recognizing the serious, irreversible harm that can come from the unregulated collection and use of biometric information, Illinois passed detailed regulations addressing the collection, use, retention, and transmission of biometric identifiers and biometric information

(together, "biometrics") by private entities, such as Defendants. A "biometric identifier" is any personal feature that is unique to an individual and includes fingerprints, iris scans, and palm scans, among others. "Biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier which is used to identify an individual. 740 ILCS 14/10.

6. In recognition of the concern over the security of individuals' biometrics and the lack of information individuals are provided regarding the same, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity, such as Defendants, may not obtain and/or possess an individual's biometrics unless it first:

> (1) informs that person in writing that biometric identifiers or biometric information will be collected or stored;
>
> (2) informs that person in writing of the specific purpose and the length of term for which such biometric identifiers or biometric information is being collected, stored and used;
>
> (3) receives a written release from the person for the collection of their biometric identifiers or biometric information; and
>
> (4) publishes a publicly available retention schedule and guidelines for permanently destroying biometric identifiers and biometric information.

740 ILCS 14/5.

7. For companies wishing to comply with BIPA, such compliance is straightforward, and the necessary disclosures and a written release can be easily achieved through a single, signed sheet of paper. BIPA's requirements bestow upon consumers a right to privacy in their biometrics and a right to make an informed decision when electing to provide or withhold their most sensitive information and on what terms.

8. BIPA's statutory scheme requires such specific disclosures prior to collecting biometrics, which in turn allows individuals the opportunity to make a truly informed choice when private entities request their biometrics. So, 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, and use biometrics and creates a private right of action for lack of statutory compliance.

9. At the time BIPA was passed in 2008, another data privacy statute, the Personal Information Protection Act, 815 ILCS § 530 *et seq*. ("PIPA"), had already been enacted in Illinois since 2006. PIPA provides a private right of action if a company possessing an individual's unique biometric data (the same data regulated by BIPA) suffers a data security breach and fails to give affected consumers proper notice of such a breach.

10. Because it believed PIPA provided insufficient protection to individuals regarding their highly sensitive biometrics, the Illinois Legislature passed BIPA to expand the law to cover not only data breach cases, but also to regulate the initial collection of such biometrics and the publication of information relating to the collection and retention of such information.

11. In this case, Defendants chose to shun less profitable timekeeping methods and instead elected to implement an invasive biometric time-tracking program that relied on the illegal collection of their workers' fingerprints to more closely monitor worker activity. Unsurprisingly, workers' privacy rights were overlooked in pursuit of corporate profits.

12. Defendants' system works by extracting biometric information from their workers' fingerprints and subsequently transferring such information to third parties, where such information is then stored and repeatedly used to track workers' time on the job.

13. Defendants implemented this biometric time-keeping regime without first obtaining the informed consent of their workers, as required by law, and all while disregarding the relevant Illinois regulations and the privacy interests they seek to protect.

14. Defendants' conduct is particularly unsettling considering the economic benefit and fraud-prevention they obtain from their biometric time-keeping system while wholly avoiding any costs associated with implementing such systems in compliance with the law. This cognizable benefit is not only to the detriment of their workers, but to their competitors as well.

15. The Illinois Legislature has found that "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, even sensitive information like Social Security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to each individual and therefore, once compromised, such individual has no recourse, is at a heightened risk for identity theft in, and is likely to withdraw from biometric facilitated transactions." 740 ILCS 14/5. The risk is compounded when, like in the employment context, a person's biometric information is also associated with their social security number and potentially other relevant financial information.

16. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendants in capturing, collecting, storing, using, and transmitting Plaintiff's biometrics, and those of hundreds of Defendants' workers throughout the state of Illinois, without informed written consent, and without informing them through a publicly available written policy of how they were going to store and dispose of this irreplaceable information, in direct violation of the Illinois BIPA.

17. Defendants' practice of collecting fingerprints from all of their workers without legal consent is unlawful and a serious invasion of their workers' right to privacy concerning their

biometrics. Defendants failed to bargain honestly with their workers in good faith at the outset of their employment relationships by failing to disclose the unlawful nature of the timekeeping system in which they would be required to participate; failed to obtain the necessary consent to transfer their workers biometrics to third parties; knowingly caused the diminution to the value of their workers' biometrics through the repeated transfer and exposure of such information to third parties; failed to maintain a lawful biometric storage program which deletes workers' information in the proscribed period; failed to provide the required disclosures to inform their workers that they were collecting their biometrics; and failed to inform them of how long they intended to keep this highly-sensitive information.

18. To the extent Defendants are still retaining Plaintiff's biometrics, such retention is unlawful and an ongoing infringement of his right to privacy regarding his biometrics. Unlike a Social Security number, which can be changed, no amount of time or money can compensate Plaintiff if his biometrics are compromised by the lax procedures through which Defendants acquire and maintain their workers' sensitive information. Plaintiff would not have provided his fingerprint to Defendants had he known that Defendants would retain such information for an indefinite period without his consent while also transferring it to third parties without his consent.

19. On behalf of himself and the proposed Class defined below, Plaintiff seeks an injunction requiring Defendants to destroy all copies and records of his biometrics in their possession and to cease all unlawful activity related to the capture, collection, storage, and use of biometrics, as well as an award of statutory damages to the Class members, together with costs and reasonable attorneys' fees.

PARTIES

20. Defendant LSC Communications, Inc. is a Delaware corporation that conducts business in Illinois. LSC is headquartered in Illinois and operates mailing and postage processing facilities through multiple subsidiaries located throughout the country, including Defendant Fairrington.

21. Defendant Fairrington, LLC is a Delaware limited liability company and subsidiary of LSC that conducts, and is licensed to conduct, business in Illinois. Fairrington is headquartered in Illinois.

22. At all relevant times, Plaintiff has been a resident and citizen of the state of Illinois and worked at one of Defendants' mail processing facilities in the Chicago area.

JURISDICTION AND VENUE

23. This Court may assert personal jurisdiction over Defendants pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendants are doing business within this state and because Plaintiff's claims arise out of Defendants' unlawful in-state actions, as Defendants captured Plaintiff's biometric data and/or biometric information in this state.

24. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101, because Defendants are doing business in Cook County and thus reside there under § 2-102, and because the transaction out of which this cause of action arises occurred in Cook County, as Defendants and/or their agents captured Plaintiff's biometrics in Cook County.

BACKGROUND

25. While most businesses track workers' time using traditional methods, such as punch clocks, Defendants' workers are expected to submit to a fingerprint scan to track their time.

Defendants accomplish this through the use of biometric timekeeping devices, which capture, collect, store, and use the Defendants' workers' fingerprints. Defendants' fingerprint scans constitute the capture and collection of biometrics for which informed consent is required prior to such capture and collection.

26. Unlike ID cards or key codes—which can be changed or replaced if stolen or compromised—fingerprints are unique and permanent identifiers of specific persons that are commonly understood to be associated with a single individual. Defendants' actions violate workers' substantive privacy rights protected under BIPA and expose Plaintiff and Defendants' other workers to serious and irreversible privacy risks.

27. As the recent Equifax Data Breach has made clear, electronically stored information (known as ESI) is notoriously difficult to protect and its dissemination can have disastrous consequences. The inherent difficulty in protecting ESI combined with the uniquely irreplaceable nature of biometric information means that the privacy risks associated with a person's biometrics are unparalleled; such information is more sensitive than a social security number, a passport, a birth certificate, etc.

28. BIPA was intended to regulate how private entities, such as Defendants, obtain individuals' biometrics; was intended to provide individuals with a statutory right to make an informed decision with respect to the circumstances in which they choose to provide their biometrics; and was also intended to regulate the possession and use of biometrics by forcing private entities under penalty to delete such biometric information within a certain period of time.

29. Specifically, BIPA requires companies to provide certain disclosures and obtain a written release from individuals *prior* to collecting their biometrics. In this way, BIPA protects individuals' right to be informed with respect to the capture, collection, storage, and use of their

biometrics, allowing them to make more informed decisions as to the circumstances under which they agree to provide their biometrics.

30. BIPA is narrowly tailored with provisions that do not place an absolute bar on the collection, capture or transmission of biometrics. However, the BIPA does provide individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their right to know the precise nature for which their biometrics are used and how they are being stored and ultimately deleted. To effectuate this purpose, BIPA mandates that entities that engage in the use of biometric systems do so with reasonable safeguards and only after receiving informed consent to take such biometrics from the individual.

DEFENDANTS' OFFENDING CONDUCT

31. Defendants' practice of capturing, collecting, transferring, converting, storing and using their workers' biometrics violates several prohibitions contained within the BIPA regulatory scheme. Defendants have failed to obtain consent from Plaintiff and the other members of the class to capture their biometrics; Defendants have failed to obtain consent from Plaintiff and the other members of the class to transfer and expose their biometrics to out-of-state third parties, including payroll processors and data storage vendors; and Defendants have failed to maintain lawful data retention practices which reduce the risk of theft or other misappropriation of their workers' biometrics by unauthorized third parties.

32. Indeed, Illinois enacted a specific and narrowly tailored law in the form of the BIPA to prevent this specific conduct from occurring by seeking to regulate entities that capture, collect, store, and use biometrics, such as fingerprints, iris scans, and handprints.

33. Defendants have failed to comply with the above-referenced BIPA regulations. By failing to comply with these regulations, Defendants deprived Plaintiff and the rest of their workers

of their right to make an informed decision with respect to the circumstances under which they choose to provide their biometrics, with such deprivation of choice and subsequent taking of biometrics constituting a severe invasion of privacy. In addition to statutory violations of BIPA, Defendants' practice of exploiting their workers' irreplaceable identities for profit violates multiple tenets of the common law.

Defendants' Fraudulent Inducement

34. Defendants and their agents negotiated work agreements with Plaintiff and the other members of the class on the basis that neither party would violate the law in the course of the employment relationship. Defendants, however, knew, or were extremely reckless in not knowing, that their biometric timekeeping program was not legally compliant. Plaintiff and the other members of the class were therefore fraudulently induced to accept and/or continue employment by being denied information about Defendants' biometric timekeeping program, by being denied the right to provide informed consent, and by Defendants' withholding of the material fact that their biometrics would be taken without their consent. Indeed, Plaintiff would not have accepted such employment, or would have sought additional compensation, had he known that Defendants' biometric timekeeping program violated Illinois law and that his biometrics would be repeatedly transferred and exposed to unknown third parties. Likewise, Plaintiff would not have accepted employment, or would have sought additional compensation, had he known that he would be required to submit his biometrics to Defendants without his lawful consent.

35. Exposure of biometrics through a data breach is an increasingly common event for even the most secure organizations. Even the U.S. government, specifically the U.S. Office of Personnel Management, which acts as the human resources department for the federal government, suffered a data breach which resulted in the theft of more than 5 million employees' fingerprints

to agents of a foreign state, the victims of which were encouraged by the federal government to immediately obtain biometric identity theft protection services to prevent unauthorized use of their biometrics.

36. Defendants were on notice that hackers regularly targeted their systems, as well as other data systems, and that their systems were therefore vulnerable to such attacks and to misappropriation by third parties. Yet, Defendants wholly failed to ensure that their biometric data collection system and process was in compliance with applicable legal standards and subjected the biometrics of their employees to the risk of such unauthorized exposure, which may have already occurred.

Defendants' Breach of Contract and Breach of the Implied Covenant of Good Faith and Fair Dealing

37. Additionally, Defendants entered into and maintained work agreements with all of their workers, including Plaintiff, and required them to use Defendants' biometric timekeeping program as a condition of their employment. Defendants, however, breached their contracts with Plaintiff and their other workers, and violated the implied covenant of good faith and fair dealing, by requiring them to participate in an unlawful biometric timekeeping program. Defendants also breached their employment contracts with their workers by taking their biometrics without their consent.

38. Plaintiff and the Class members entered into and/or were the beneficiaries of employment contracts with Defendants. These contracts were subject to the implied covenant of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and would not impair the rights of the other parties to receive their rights, benefits, and reasonable expectations under the contracts. This obligation included the covenant that the Defendants would act fairly, reasonably,

and in good faith in bargaining the employment agreements between themselves and Plaintiff and the Class members.

39. Defendants did not act fairly in this bargaining process because they withheld information regarding their biometric timekeeping system, including the nature of the system and how the biometric information was to be collected, stored, transmitted, and ultimately deleted, as well as the fact that, under the law, Plaintiff and the other Class members had an absolute right to provide informed consent as to their participation in such a biometric program.

40. Defendants were in sole possession of such information, and Plaintiff and the other workers reasonably relied on Defendants not only to conduct a timekeeping program in compliance with the law generally, but to provide them with the necessary and appropriate information as required by the law.

41. Even if Defendants are held not to have breached any express promise in these employment contracts, Defendants breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the confidentiality of Plaintiff's and the other Class members' biometrics, resulting in the exposure and transfer of Plaintiff's biometrics to third parties.

42. Defendants unreasonably interfered with the contract benefits owed to Plaintiff and Class members by, among other things, compiling and storing Plaintiff's and the other Class members' biometrics in databases accessible to multiple vendors and failing to implement reasonable auditing procedures to detect and halt the dissemination of biometrics without Plaintiff and the other Class members' consent.

43. Plaintiff and Class members performed all conditions, covenants, obligations, and promises owed to Defendants, including working on all required occasions and providing Defendants their confidential biometrics. As a result of Defendants' breach of contract, including

breach of the implied covenant of good faith and fair dealing, Plaintiff and the Class members did not receive the full benefit of their bargain, and instead received employment under terms that that were less valuable than their reasonable expectations under their contracts.

Defendants' Negligence

44. To the extent that a finder of fact concludes that Defendants did not intentionally and knowingly withhold material information from Plaintiff and the Class members relating to their biometric timekeeping program and the consent to obtain biometrics required under BIPA, Defendants were careless and negligent in their failure to comply with BIPA and their failure to provide Plaintiff and the other workers with the information required by statute and necessary to provide informed consent as to the terms of providing such biometrics and the terms of entering into such an employment relationship.

45. In reliance upon these misrepresentations or omissions, Plaintiff and the other Class members accepted employment by Defendants without important information that would have been material to Plaintiff and the Class members' decision to provide their biometrics and to enter into the employment relationship with Defendants. Had Plaintiff and the other Class members, as reasonable persons, known that Defendants were failing to comply with the requirements of state law pertaining to the privacy and security of Class members' biometrics, they would not have accepted employment by Defendants in exchange for the consideration provided, and would not have entrusted Defendants with their biometrics.

46. As a direct and proximate consequence of Defendants' negligent misrepresentations, Plaintiff and the other Class members have suffered lost wages and diminution in the unique identifying value of their biometric information caused by Defendants' repeated

transfer and exposure of such information to multiple out-of-state, third-party payment processors and data storage vendors, among others.

47. Additionally, Defendants knew, or should have known, of the risks inherent in collecting and storing its workers' biometrics and owed duties of reasonable care to Plaintiff and the Class members whose biometrics were obtained through their employment by Defendants.

48. Defendants breached their duties to Plaintiff and the Class members by failing to implement a BIPA-compliant biometric timekeeping system with reasonable data security safeguards.

Defendants' Negligence Per Se

49. Pursuant to BIPA, Defendants had a duty to maintain reasonable security procedures and practices to secure Plaintiff's and the Class members biometrics. Defendants breached that duty by failing to obtain consent to capture Plaintiff's and the Class members' biometrics and to prevent the transfer of such information to third parties without their consent or knowledge.

50. Defendants' failure to comply with applicable laws such as BIPA constitutes negligence per se. The injury and harm suffered by Plaintiff and the other Class members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would constitute the withholding of informed consent and would cause Plaintiff and the other Class members to experience the foreseeable harms associated with the exposure of their biometrics to third parties and the foreseeable harms associated with the taking of their biometrics without their consent.

51. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and the other Class members, Plaintiff and the other Class members would not have been injured.

Defendants' Intrusion Upon Seclusion

52. In Illinois, one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

53. The illegal taking of biometrics in the form of fingerprints without a person's consent constitutes an intrusion that would be highly offensive to a reasonable person. Similarly, the unauthorized transmission of such information to unknown third parties without knowledge or consent of the individual whose biometrics are transferred constitutes another intrusion that would be highly offensive to a reasonable person.

54. Defendants, through the use of their biometric scanning devices, illegally captured and transmitted Plaintiff's and other Class members' biometrics without consent, thereby intruding on their right to privacy with respect to their biometrics.

Taking of Biometrics Without Consent Constitutes Informational Injury

55. The Federal Trade Commission ("FTC") recently hosted a workshop to discuss the topic of "informational injury."[1] Consumers suffer an informational injury when information about them is misused or otherwise illegally obtained, as is the case when companies violate BIPA.

56. As stated by acting FTC Chairman Maureen K. Ohlhausen in her opening remarks to the Informational Injury Workshop, the workshop addressed, among other issues, the range of injuries that occur from privacy and data security incidents, including "unwarranted health and

[1] *See FTC Informational Injury Workshop*, December 12, 2017 (full workshop video, transcripts, and materials available at https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop).

safety risk" and "intrusion into seclusion," in addition to the "direct financial injuries" that can occur; and how do consumers weigh the benefits and costs of sharing information." The FTC is aware of the growing use of sensitive consumer information and the importance of recognizing and quantifying the cognizable data privacy injury that consumers suffer in addition to direct financial harms when such information is unlawfully acquired, used, or otherwise obtained.

57. Panelist Giner Jin, former Director of the FTC's Bureau of Economics, discussed the limitations of measuring informational injury from an *ex-post* perspective because "a lot of harm may not happen yet, but there's risk there . . . emphasis on *ex-post* harm . . . ends up encouraging overuse or misuse of data." Jin advocated the use of the *ex-ante* perspective due to its emphasis "on the increase of risk of harm to consumers, even if that risk has not been realized[.]"

58. According to panelist Lynn Langston, who oversees the National Crime Victimization Survey, which is one of two measures of crime in the U.S., "even among identity theft victims, that experience no financial losses – so they have no financial losses whatsoever – there are still harms . . . about 30% still found the incident to be moderately to severely distressing. So that suggests in and of itself, the experience of having your information misused . . . your information out there[,] has some harm to victims."

59. Leading professionals in the arena of consumer protection and data privacy recognize that such injuries are not confined to direct pecuniary harms. Real harm may occur long before a data breach, and real harm is not contingent on a data breach, not limited to the *ex-post* perspective, and may manifest itself as not receiving the benefit of contractual bargain, the destruction of one's own sense of security and comfort in their data privacy**,** mental distress as a

result of involuntary subjection to an increased risk of identity theft, and direct pecuniary harm, among other cognizable injuries.

60. As a direct and proximate cause of Defendants' conduct, and as alleged in greater detail herein, Plaintiff suffered all or some of the aforementioned informational injuries discussed during the FTC Informational Injury Workshop.

61. An article published in the *New York Times* succinctly explains the serious risks in detail and how large businesses, like Defendants, are at risk of a data breach:

> Hacking of banks and identities is big business. An estimated 17.6 million Americans were subject to identity theft in 2014, mostly through breached bank accounts and credit cards. At this point, bank hackers are probably not looking for biometric data when attacking a bank. But even if it leaks as a by-product of a financial breach, criminals will find ways to abuse biometric data or resell it for further exploitation. And biometric data is more sensitive than other personal information banks store on behalf of their customers because unlike a credit card number (or even a name!), stolen biometric data cannot be replaced: It corresponds to a person's face or fingerprints….
>
> **If the compromised data happens to be biometrics, issues of identity theft may simply be unresolvable**. … It is not enough for banks to simply avoid storing images of fingerprints, faces or irises. The biometric data that they get from processing those geometries (what banks call "templates") can also be abused if they are accessed in combination with the algorithm used to extract the templates from the original images.[2]

FACTS SPECIFIC TO PLAINTIFF

62. During the relevant time period, Plaintiff worked at a facility owned and operated by Defendants and located in Chicago, Illinois.

63. At this facility, Defendants' time keeping practice has relied on a biometric scanning device which scans workers' fingerprints to track the workers' time.

[2] Yana Welinder, *Biometrics in Banking Is Not Secure*, The New York Times, July 13, 2016 (available at http://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-in-banking-is-not-secure) (last visited January 31, 2018) (emphasis added).

64. Defendants acquired and installed several biometric timekeeping devices at their facilities and required their workers, including Plaintiff, to have their fingerprints scanned by their biometric timekeeping devices, which captured, collected, and stored the fingerprints. Defendants' workers' biometric identifiers were associated with their identities and used by Defendants to identify and track their work time. Additionally, Defendants installed this technology on its premises and required its workers to use it in order to extract greater profit which occurred at the expense of its workforce's right to privacy in their biometrics.

65. After workers' biometrics are captured and collected by the Defendants, Defendants require such workers to scan their fingers using Defendants' biometric timekeeping devices each time they "clock-in" and "clock-out." Defendants' system ensures that workers can only verify their attendance and timeliness through scanning such information.

66. In addition to the instance when workers' fingerprints are initially captured, on each occasion that Defendants' workers in Illinois scan a finger through Defendants' biometric timekeeping devices, Defendants are capturing and using workers' biometrics without regard to Illinois' statutory requirements under the BIPA and thereby invading the workers' privacy. Defendants then transmit such biometrics to out-of-state payroll processors and other vendors, who then store and use such information on each successive occasion it is provided by Defendants.

67. Prior to taking Plaintiff's biometrics, Defendants did not inform Plaintiff in writing that his biometrics were being collected, stored, or used, nor did Defendants publish any policy about the collection, retention, and use of such information. Defendants did not seek, and Plaintiff never provided, any written consent relating to the collection, use, storage, or transmission of his biometrics.

68. Prior to taking Plaintiff's biometrics, Defendants did not make publicly available any written policy as to a biometric retention schedule and guidelines for permanently destroying the collected biometrics, as required by the BIPA.

69. Additionally, Defendants did not obtain consent from Plaintiff or its workers for any transmission of their biometrics to third parties. Defendants have violated the BIPA on each occasion they transmit such biometrics to third parties.

70. To this day, Plaintiff is unaware of the status of his biometric obtained by Defendants. Defendants have not informed Plaintiff whether they still retain his biometrics, and if they do, for how long they intend to retain such information without his consent. Plaintiff has suffered pecuniary damages in the form of lost wages, diminution in the unique identifying value of his biometrics, and attorneys' fees and costs incurred to redress such harms. Furthermore, Plaintiff's biometrics are economically valuable and such value will increase as the commercialization of biometrics continues to grow. Defendants' repeated use of Plaintiff's biometrics does and will continue to confer a benefit on Defendants for which he was not sufficiently compensated. Additionally, Plaintiff has spent significant time, effort and expense assessing biometric fraud, monitoring his accounts, and addressing issues arising from Defendants' unlawful use of his biometrics.

71. Defendants do not have a policy of informing their workers in any way what happens to their biometrics after they are 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 Defendants, if a facility were to close, or if Defendants were to be acquired, sold, or file for bankruptcy. Such sales and acquisitions are common in

Defendants' industry. Indeed, during the relevant period, the assets of Defendant Fairrington, including its workers' fingerprint data, were acquired by Defendant LSC.[3]

72. As a result of Defendants' conduct, Plaintiff has also experienced injury in the form of mental anguish and anxiety. Plaintiff has experienced mental anguish and injury when he thinks about the status of his biometrics and who has had, or could have, access to such private information; what would happen to his biometrics if Defendants or their vendors went bankrupt or otherwise sold their assets; when he wonders whether Defendants will ever delete his biometric information; and when he wonders what would happen to his information and identity if Defendants or their vendors were to experience a data breach.

73. This harm is even more acute because an individual with access to Plaintiff's biometrics could potentially access other financial accounts or health records which may currently, or at some time in the future, be secured through his biometrics. He experiences similar anguish when thinking about the fact that his information was taken from him unlawfully. Plaintiff's concern is magnified by the fact that Defendants not only obtained scans of his fingerprint in violation of the law, but also associated such information with his identity.

74. By knowingly and willfully failing to comply with the BIPA's mandatory notice, consent, retention, transmission, and policy publication requirements, Defendants have violated Plaintiff's and other workers' substantive privacy rights protected under the BIPA. Plaintiff and the other members of the Class have continuously been exposed to substantial and irreversible loss of privacy by Defendants' conduct, constituting a severe harm and violation of their rights.

[3] *See LSC Communications Acquires Fairrington Transportation,* available at http://www.piworld.com/article/lsc-acquires-fairrington-transportation, (last visited January 31, 2018).

CLASS ALLEGATIONS

75. Plaintiff brings this action on behalf of himself and similarly situated individuals pursuant to 735 ILCS § 5/2-801. Plaintiff seeks to represent a Class defined as follows:

> All individuals whose biometric identifiers and/or biometric information were captured, collected, obtained, stored or used by Defendants within the state of Illinois any time within the applicable limitations period.

76. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendants; and any immediate family member of such officer or director.

77. Upon information and belief, there are over one hundred 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 Defendants' personnel records.

78. Plaintiff's claims are typical of the claims of the Class members he seeks to represent, because the factual and legal bases of Defendants' liability to Plaintiff and the other Class members are the same, and because Defendants' conduct has resulted in similar injuries to Plaintiff and to the Class. As alleged herein, Plaintiff and the other putative Class members have all suffered damages as a result of Defendants' BIPA violations and various common law transgressions.

79. There are many questions of law and fact common to the claims of Plaintiff and the other Class members, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendants collect, capture, store, use, and/or transfer the

biometrics of Class members;

b. Whether Defendants developed and made available to the public a written policy which establishes a retention schedule and guidelines for permanently destroying biometrics;

c. Whether Defendants obtained a written release from Class members before capturing, collecting, or otherwise obtaining workers' biometrics;

d. Whether Defendants provided a written disclosure to their workers that explains the specific purposes, and the length of time, for which their biometrics were being collected, stored and used before taking their biometrics;

e. Whether Defendants' conduct violates the BIPA;

f. Whether Defendants' conduct is fraudulent;

g. Whether Defendants' conduct is negligent;

h. Whether Defendants' conduct constitutes an invasion of privacy;

i. Whether Defendants' violations of the BIPA are willful and reckless; and

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

80. 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 or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

81. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class he seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his 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 his counsel has any interest adverse to those of the other members of the Class.

82. Defendants have acted and failed to act on grounds generally applicable to the Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNTS I-VI

Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*.,
(on behalf of Plaintiff and the Class)

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

84. Defendants are "private entities" under BIPA.

85. Plaintiff and the other Class members had their "biometric identifiers," namely their fingerprints, collected, captured, received or otherwise obtained by Defendants. Plaintiff's and the other Class members' biometric identifiers were also used to identify them, and therefore constitute "biometric information" as defined by the BIPA. 740 ILCS 14/10.

86. Each instance when Plaintiff and the other Class members scanned their fingers into Defendants' timekeeping devices, Defendants captured, collected, stored, and/or used Plaintiff's and the Class members' biometrics without valid consent and without complying with BIPA.

87. Defendants' practice with respect to capturing, collecting, storing, and using biometrics fails to comply with the applicable BIPA requirements. Specifically, with respect to Plaintiff and the other Class members, Defendants failed to adhere to the following BIPA requirements, with each such failure constituting a separate and distinct violation of BIPA and a separate and distinct cause of action:

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

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

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

e. Defendants failed to provide a publicly available retention schedule detailing the length of time biometric were stored and/or guidelines for permanently destroying the biometrics it stores, as required by 740 ILCS 14/15(a); and

f. Defendants failed to obtain consent to disclose or disseminate the Class members' biometrics, as required by 740 ILCS 14/15(d)(1).

88. By capturing, collecting, storing, using, and transmitting Plaintiff's and the other Class members' biometrics as described herein, Defendants violated Plaintiff's and the other Class members' respective rights to privacy concerning their biometrics, as set forth in BIPA.

89. Had Defendants informed Plaintiff at the time he accepted employment that he was not being provided all information regarding his biometrics and Defendants' biometric time-keeping program as required by law, he would not have accepted employment with Defendants or he at least would have sought additional compensation.

90. Had Defendants informed Plaintiff at the time he accepted employment that he would be asked to participate in an illegal biometric time-keeping program, he would not have accepted employment with Defendants at the offered rate of compensation, or he at least would have been able to make an informed decision concerning material facts of his employment, including whether the rate of pay and opportunity cost justify participating in Defendants' unlawful biometric program.

91. Had Defendants complied with the BIPA and provided Plaintiff with all statutorily-required disclosures, he would have been able to make an informed decision regarding the circumstances of his employment, including whether to accept the offered rate of pay, whether to request concessions or other accommodations related to participation in Defendants' biometric program, whether to condition his employment on being provided with an alternative timekeeping mechanism which did not depend on the provision of my sensitive biometric information, and whether the rate of pay and opportunity cost justify participating in Defendants' biometric program, and Plaintiff would have sought additional compensation.

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

93. Defendants' violations of BIPA, as set forth herein, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with the BIPA disclosure, consent, and policy posting requirements.

COUNT VII
Fraudulent Inducement
(on behalf of Plaintiff and the Class)

94. Plaintiff hereby incorporates Paragraphs 1 through 43 and 52 through 93 by reference as if fully set forth herein.

95. Defendants negotiated employment agreements with Plaintiff and the other members of the class on the basis that neither party would violate the law in the course of the employment relationship.

96. Defendants, however, knew, or were reckless in not knowing, that their biometric timekeeping program was not legal and fraudulently induced Plaintiff and the other Class members to accept and/or continue employment by denying them information that was material and legally required to be disclosed, about Defendants' biometric timekeeping program; by denying them the right to provide informed consent for participation in the biometric timekeeping program and the collection and use of their respective biometrics; and by failing to disclose the fact that their biometrics would be taken without their consent and transmitted to third parties without their knowledge or consent.

97. The information set forth above was material to Plaintiff and the other Class members because it was necessary to make an informed decision as to the participation in

Defendants' biometric timekeeping program and was material to the decision as to whether to accept and/or continue employment and at what compensation. Indeed, Plaintiff would not have accepted such employment at the rate he was paid had he known that Defendants' biometric timekeeping program violated Illinois law and that his biometrics would be repeatedly transferred and exposed to unknown third parties.

98. By intentionally withholding such material and statutorily-required information, Defendants induced Plaintiffs and the other Class members to enter into and/or continue their employment relationships with Defendants on false and misleading terms and allowed Defendants' to obtain access to the biometrics of Plaintiff and the other Class members on false pretense.

99. Plaintiff and the other Class members were fraudulently induced by Defendants' material omissions and were injured in an amount to be determined at trial by being denied access to necessary information, by being denied their right to provide informed consent for the provision of their biometrics, and by entering into employment contracts on such terms that would not have existed but for Defendants' intentional omissions of material fact.

COUNT VIII
Breach of Contract and the Implied Covenant of Good Faith and Fair Dealing
(on behalf of Plaintiff and the Class)

100. Plaintiff hereby incorporates by reference the foregoing allegations as if fully set forth herein.

101. Plaintiff and the Class members entered into and/or were the beneficiaries of employment contracts with Defendants. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and to negotiate such contracts in good faith.

102. Defendants failed to negotiate in good faith by not disclosing information regarding their collection of biometrics that they were statutorily obligated to provide prior to such collection. This failure was material to the employment relationship and affected Plaintiff's and other workers' decision-making process.

103. Had Defendants informed Plaintiff at the time he accepted employment that he was not being provided all information regarding his biometrics and Defendants' biometric time-keeping program as required by law, he would not have accepted employment with Defendants or he at least would have sought additional compensation.

104. Had Defendants informed Plaintiff at the time he accepted employment that he would be asked to participate in an illegal biometric time-keeping program, he would not have accepted employment with Defendants at the offered rate of compensation, or he at least would have been able to make an informed decision concerning material facts of his employment, including whether the rate of pay and opportunity cost justify participating in Defendants' unlawful biometric program.

105. Had Defendants complied with the BIPA and provided Plaintiff with all statutorily required disclosures, he would have been able to make an informed decision regarding the circumstances of his employment, including whether to accept the offered rate of pay, whether to request concessions or other accommodations related to participation in Defendants' biometric program, whether to condition his employment on being provided with an alternative timekeeping mechanism which did not depend on the provision of my sensitive biometric information, and whether the rate of pay and opportunity cost justify participating in Defendants' biometric program, and Plaintiff would have sought additional compensation.

106. Defendants also unreasonably interfered with the contract benefits owed to Plaintiff and Class members by compiling and storing Plaintiff and the other Class members' biometrics in databases accessible to multiple vendors without the informed consent of such individuals.

107. Plaintiff and the Class members performed all conditions, covenants, obligations, and promises owed to Defendants, including working when required and providing Defendants the required sensitive and confidential biometrics. As a result of Defendants' breach of contract, including breach of the covenant of good faith and fair dealing, Plaintiff and the Class members did not receive the full benefit of their bargain.

108. As a result of Defendants' breach of contract, including breach of the covenant of good faith and fair dealing, Plaintiff and the other Class members have also suffered actual damages resulting from the exposure of their biometrics to third parties and remain at risk of suffering additional damages in the future.

109. Plaintiff and the Class members were damaged in an amount at least equal to the difference in value between that which they reasonably expected under the contract and Defendants' partial, deficient and/or defective performance.

110. As a result of Defendants' breach of contract, including breach of the implied covenant of good faith and fair dealing, Plaintiff and the Class members have suffered actual damages resulting from their attempt to ameliorate the effect of the breach and the subsequent loss of exclusive control and possession of their biometrics, including but not limited to purchasing credit monitoring services and taking other steps to protect themselves from the unlawful taking of their biometrics.

111. Accordingly, Plaintiff and Class members have been injured as a result of Defendants' breach of contract, including breach of the covenant of good faith and fair dealing, and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IX
Negligence
(on behalf of Plaintiff and the Class)

112. Plaintiff hereby incorporates by reference the foregoing allegations as if fully set forth herein.

113. Alternatively, to the extent that it is determined that Defendants did not intentionally and knowingly withhold material information from Plaintiff and the Class members relating to their biometric timekeeping program and the consent to obtain biometrics required under BIPA, Defendants were nonetheless careless and negligent in their failure to comply with BIPA and to provide Plaintiff and the other Class members with the information required by statute and necessary to provide informed consent as to the terms of providing such biometrics and the terms of entering into an employment relationship with Defendants.

114. A "special relationship" also exists between Defendants and Plaintiff and the other Class members because Defendants are or were employers of Plaintiff and the other Class members and thus stand in a fiduciary or quasi-fiduciary relationship with Plaintiff and the other Class members and had full control over the collection, use, storage, and transfer of their sensitive and confidential biometrics.

115. In reliance upon Defendants' misrepresentations, Plaintiff and the other Class members accepted employment by Defendants in the absence of information about the biometric timekeeping program that was material to their decision to participate in the program and/or to accept or continue employment on the terms offered by Defendants. Had Plaintiff and the other

Class members, as reasonable persons, known Defendants' were failing to comply with the requirements of state law pertaining to the privacy and security of Class members' biometrics, they would not have accepted employment by Defendants in exchange for the consideration provided, and would not have entrusted their biometrics to Defendants.

116. As a direct and proximate consequence of Defendants' negligent misrepresentations, Plaintiff and the other Class members have suffered lost wages and diminution in the unique identifying value of their biometrics caused by Defendants' transfer and exposure of such information to multiple out-of-state, third-party payment processors, including ADP, and data storage vendors, among others.

117. Additionally, Defendants knew, or should have known, of the risks inherent in collecting and storing the biometrics of their workers and owed duties of reasonable care to Plaintiff and the Class members whose biometrics were obtained through their employment by Defendants. Additionally, Defendants knew or should have known that hackers would attempt to access information in the corporate databases of Defendants.

118. Defendants breached their duties to Plaintiff and the Class members by failing to provide fair, reasonable, adequate, and sufficient biometric information privacy systems to safeguard Plaintiff's biometrics.

119. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiff and the other Class members to experience the foreseeable harms associated with the exposure of their biometrics to third parties, including the discontinuation of Plaintiff's exclusive possession and control of his biometric biometrics and the accompanying loss of the unique identifying value of his biometrics.

120. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and the Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT X
Negligence *Per Se*
(On behalf of Plaintiff and the Class)

121. Plaintiff hereby incorporates by reference the foregoing allegations as if fully set forth herein.

122. Pursuant to 740 ILCS 14/10, Defendant:

a. Had a duty to inform Plaintiff and the members of the Class in writing that their biometrics were being collected and stored, as required by 740 ILCS 14/15(b)(1);

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

c. Had a duty to inform Plaintiff and the members of the Class in writing of the specific length of term their biometric identifier or biometric identifiers were collected, stored and used, as required by 740 ILCS 14/15(b)(2);

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

e. Had a duty to provide a publicly available retention schedule detailing the length of time biometric identifiers and biometric information is stored or guidelines for permanently destroying the biometrics it stores, as required by 740 ILCS 14/15(a); and

f. Had a duty to obtain consent to disclose or disseminate the Class members' biometrics, as required by 740 ILCS 14/15(d)(1).

123. Defendants breached each and every one of the aforementioned duties.

124. Defendants' failure to comply with the duties set forth in BIPA constitutes negligence *per se.*

125. But for Defendant's wrongful and negligent breaches of their duties owed to Plaintiff and the Class members, Plaintiff and the Class members would not have been injured, including but not limited to the denial of their access to information that was material to their ability to provide informed consent as to their participation in Defendants' biometric timekeeping program, the providing of their biometrics, and their acceptance of employment at the terms offered by Defendants.

126. Defendants' negligence also resulted in injury in the form of exposure of Plaintiff's and the Class members' biometrics to third parties without their knowledge or consent, as well as the discontinuation of Plaintiff's and the Class members' exclusive possession and control of their biometrics and accompanying loss of the unique identifying value of their biometrics.

127. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or should have known that they were failing to meet their duties to Plaintiff and the Class members and that Defendants' breaches would cause Plaintiff and the Class members to experience the foreseeable harms associated with the unauthorized capture, use, possession, storage, and transmission of their biometrics.

128. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT XI
Intrusion Upon Seclusion
(On behalf of Plaintiff and the Class)

129. Plaintiff hereby incorporates the foregoing paragraphs as if fully set forth herein.

130. Defendants have intentionally and unlawfully intruded upon Plaintiff's and the Class members' private affairs and concerns by using biometric scanning devices to physically collect their biometrics without receiving consent, despite the fact that consent is required by law.

131. Defendants have intentionally and unlawfully intruded upon Plaintiff's and the Class members' private affairs and concerns by failing to inform them of the specific purpose and length of term for which they intended to retain and use their biometrics, despite the fact that such disclosures are required by law.

132. Defendants have intentionally and unlawfully intruded upon Plaintiff's and the Class members' private affairs and concerns by transmitting their biometrics to unknown third parties without knowledge or consent, despite the fact that information about, and consent for, such transmission to third parties is required by law.

133. Plaintiff and the Class members had a reasonable expectation that any entity seeking to collect their biometrics, but particularly their employer, would be doing so in accordance with the law.

134. A reasonable person would find it highly offensive and objectionable that an entity would intrude on their highly sensitive and irreplaceable biometrics in violation of the law and without his/her legal consent, and Plaintiff and the Class members did find Defendants' conduct to be both highly offensive and objectionable.

135. These repeated intrusions caused damages to Plaintiff and the other Class members in the form of, among other things, mental anguish, and Plaintiff and the Class members seek monetary damages and restitution in an amount to be determined at trial.

PRAYER FOR RELIEF

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

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

b. Declaring that Defendants' actions, as set forth herein, violate the BIPA;

c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendants to comply with the BIPA requirements for the capture, collection, storage, use, and transmission of biometric identifiers and biometric information, including an injunction requiring Defendants to permanently destroy all biometric information of Plaintiff and of Class members in their possession and compensation in an amount to be determined at trial for the commercial value of Plaintiff's biometric information;

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(1);

e. Awarding statutory damages of $1,000 for each negligent violation of the BIPA, pursuant to 740 ILCS 14/20(3);

f. Awarding monetary damages and equitable relief for Defendants' fraudulent conduct, breach of contract, negligence, negligence *per se*, and intrusion upon seclusion in an amount to be determined at trial;

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

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

i. 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: February 1, 2018

Respectfully Submitted,

RAY MCGEE, individually and on
behalf of a class of similarly situated individuals

By: /s/ David L. Gerbie
One of Plaintiff's Attorneys

Evan M. Meyers
David L. Gerbie
Jad Sheikali
MCGUIRE LAW, P.C. (Firm ID 56618)
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
Fax: (312) 275-7895
emeyers@mcgpc.com
dgerbie@mcgpc.com
jsheikali@mcgpc.com

Attorneys for Plaintiff and the Putative Class