# EXHIBIT 1

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

| | | |
|---|---|---|
| **MICHELE JOHNSON and CHRISTINA SKELDON, individually, and on behalf of all others similarly situated,** | ) | |
| **Plaintiffs,** | ) | **Case No.** 2022CH04265 |
| **v.** | ) | |
| **NCR CORPORATION,** | ) | |
| **Defendant.** | ) | |

## CLASS ACTION COMPLAINT

Plaintiffs Michele Johnson ("Johnson") and Christina Skeldon ("Skeldon") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated (the "Class"), by and through their attorneys, bring the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against NCR Corporation ("NCR" or "Defendant"), its subsidiaries and affiliates, to redress and curtail Defendant's unlawful collection, obtainment, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric identifiers and biometric information (collectively referred to herein as "biometric data"). Plaintiffs allege as follows upon personal knowledge as to themselves, their own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by their attorneys.

## NATURE OF THE ACTION

1. Defendant NCR is a vendor of hardware, software, and service solutions intended to power businesses across a wide swath of sectors, including banking, telecommunications, retail, and restaurants.

2. Chief among the products that NCR develops, manufactures, and sells to its customers in the restaurant industry include biometric-enabled Point-of-Sale ("POS") systems, which are comprised of POS terminals, like the NCR CX5[1], and cloud-based POS software, like NCR Aloha[2].

3. NCR develops and markets its POS systems as an "all-in-one" solution, configuring its POS software solutions so that they feature various applications capable of performing essential management functions, including tracking and managing workers' time and attendance.

4. Each NCR POS terminal model is configured so that it can be used in conjunction with a biometric fingerprint scanner.

5. When an NCR POS terminal is configured to be biometric-enabled using a biometric fingerprint scanner, a worker is required to scan his or her fingerprint at the biometric-enabled NCR POS system in order to access the terminal, whether to clock-in or clock-out or to input a food order.

6. Typically, biometric devices function by capturing an image of a worker's fingerprint when the worker enrolls at the biometric device. From the image, unique features of the fingerprint are extracted to create a unique template associated with the worker, which is stored in an NCR database. Each time the worker subsequently provides his or her fingerprint at the biometric device, the device compares the unique features of the input fingerprint against the stored templates of each set of fingerprints enrolled to verify the worker's identity.

---

[1] *See POS hardware solutions for restaurants*, NCR, *available at* https://www.ncr.com/restaurants/restaurant-hardware (last accessed May 2, 2022).

[2] *NCR's Aloha Restaurant POS System gives you everything you need to manage your restaurant fearlessly*, NCR, *available at* https://www.ncr.com/restaurants/aloha-restaurant-pos-system (last accessed May 2, 2022).

7. When an employer opts to use the time and attendance application on a biometric-enabled NCR POS system, workers' biometric data captured at the employer's biometric-enabled POS system is automatically uploaded to an NCR database, where it is managed, maintained, and stored on NCR's hosted environments and servers.

8. NCR collected and/or otherwise obtained workers' biometric data captured by the biometric-enabled POS terminals optimized with NCR's POS software, including but not limited to NCR Aloha.

9. Despite its collection of biometric data from workers whose employers utilize its services, NCR fails to secure informed consent from subjects of collection, authorizing it to collect, store, use, or disclose their biometric data.

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

11. While there are benefits to using biometric timekeeping devices in the workplace, there are also serious risks. Unlike key fobs or identification cards—which can be changed or replaced if stolen or compromised—fingerprints are unique, permanent biometric identifiers associated with each individual. This exposes individuals like Plaintiffs 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 Clearview AI, Facebook/Cambridge Analytica, and Suprema data breaches—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. An illegal market exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data—including fingerprints, iris scans, and facial photographs—of over a billion Indian citizens.[3] 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.[4]

13. 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, obtain, store, and use Illinois citizens' biometric data.

14. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregards Illinois workers' statutorily protected privacy rights and unlawfully collects, obtains, stores, disseminates, and uses their biometric data in violation of BIPA. Specifically, Defendant has violated and continues to violate BIPA because it did not:

a. Properly inform Plaintiffs and others similarly situated in writing of the specific purpose and length of time for which their biometric data was being collected, obtained, stored, and used, as required by BIPA;

b. Obtain a written release from Plaintiffs and others similarly situated to collect, obtain, store, disseminate, or otherwise use their biometric data, as required by BIPA;

c. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiffs' and other similarly-situated individuals' biometric data, as required by BIPA; and

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

---

[3] *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-identitytheft/?utm_term=.b3c70259fl38.

[4] Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), *available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

15. Accordingly, Plaintiffs seek an Order: (1) declaring that Defendant's conduct violates BIPA; (2) requiring Defendant to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiffs and the proposed Class.

## PARTIES

16. Plaintiff Michele Johnson is a natural person and a citizen of the State of Illinois.

17. Plaintiff Christina Skeldon is a natural person and a citizen of the State of Illinois.

18. Defendant NCR Corporation is a Maryland corporation that conducts business in the State of Illinois.

## JURISDICTION AND VENUE

19. This Court has jurisdiction over Defendant NCR pursuant to 735 ILCS § 5/2-209 because Defendant conducts business transactions in the State of Illinois, including at its Aloha POS retail store located at 9701 W. Higgins Road, Suite 120, Rosemont, Illinois 60018, committed the statutory violations alleged herein in Illinois, and is registered to conduct business in Illinois.

20. Venue is proper in Cook County because Defendant conducts business in this State, conducts business transactions in Cook County, and committed at least some of the statutory violations alleged herein in Cook County, Illinois.

## FACTUAL BACKGROUND

### I. The Biometric Information Privacy Act

21. 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.

22. 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 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.

23. 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.

24. 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.

25. BIPA is an informed consent statute that achieves its goal by making it unlawful for a company to, among other things, collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

a. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored, and used;

b. Informs the subject in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, obtained, 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).

26. BIPA defines a "written release" as "informed written consent." 740 ILCS § 14/10.

27. Biometric identifiers include fingerprints, retina and iris scans, voiceprints, and scans of hand and face geometry. *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.*

28. BIPA 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 disclosure. *See* 740 ILCS § 14/15(d)(1).

29. 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).

30. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and—

most significantly—the unknown ramifications of biometric technology. Biometrics are biologically unique to the individual, and, once compromised, an individual is at heightened risk for identity theft and left without any recourse.

31. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, obtain, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

32. Plaintiffs, like the Illinois legislature, recognize how imperative it is to keep biometric identifiers and biometric information secure. Biometric data, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

## II. Defendant Violates the Biometric Information Privacy Act.

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

34. However, NCR failed to take note of the shift in Illinois law governing the collection, obtainment, storage, use, and dissemination of biometric data. As a result, NCR continues to collect, obtain, store, use, and disseminate Illinois citizens' biometric data in violation of BIPA.

35. NCR's biometric hardware and software, like other biometric technology, authenticate workers' identities by capturing and utilizing their biometric identifiers and/or information.

36. Specifically, when workers first use a biometric-enabled NCR POS system, they are required to have their fingerprint scanned in order to enroll them in an NCR database(s), from which NCR collects and/or otherwise obtains workers' biometric data. Thereafter, NCR again collects and/or otherwise obtains workers' fingerprint data upon each subsequent scan of the workers' fingerprint to clock-in and clock-out of work or to otherwise access the POS terminal.

37. All biometric-enabled NCR POS systems are designed and constructed with a network interface, which provides for transmission of biometric data collected and/or obtained from biometric-enabled NCR POS systems to NCR's servers and to third-parties who host that data.

38. NCR discloses workers' biometric data to third-parties, which receive, store, use, access, or otherwise process the biometric data for the purpose of providing their services, including the back-up storage of data and provision of IT services.

39. NCR developed and markets cloud-based software platforms, like NCR Aloha, through which NCR actively manages, maintains, and stores data collected from its biometric-enabled POS terminals, including biometric data, in a single, centralized location on its hosted environments and servers.

40. NCR accesses its servers, where data collected from its POS terminals is stored, for various purposes, including to provide support services to its employer-customers.

41. NCR fails to sufficiently inform workers enrolled with its biometric-enabled POS systems: that NCR is collecting, obtaining, storing, disseminating, or using their sensitive biometric data; the extent or the purposes for which it does so; or to whom the data is disclosed.

42. Defendant NCR fails to sufficiently inform workers that, through its biometric-enabled POS terminals and cloud-based POS software, it collects, maintains, stores, disseminates,

and uses their biometric data; fails to inform workers that it discloses or disclosed their biometric data to other, currently unknown, third parties, which host the biometric data in their data centers; fails to properly inform workers of the purposes and duration for which it collects their sensitive biometric data; and fails to obtain written releases from workers before collecting, obtaining, and/or disseminating their biometric data.

43. Defendant did not create or maintain a written, publicly available policy identifying its retention schedule and guidelines for permanently destroying Plaintiffs' and other similarly-situated individuals' biometric data and did not and will not destroy Plaintiffs' and other similarly-situated individuals' biometric data when the initial purpose for collecting, capturing, or obtaining such data had been satisfied or within three years of the worker's last interaction with the company.

44. NCR profits from the use of workers' biometric data. For instance, NCR markets and distributes its biometric-enabled POS terminals and cloud-based software platforms to Illinois employers as a superior option to traditional POS solutions because it leverages scans of workers' biometric identifiers to create a verifiable, user-unique audit trail that can facilitate authentication and monitoring of POS terminal access and accurate time collection to help deter costly "buddy punching"—where one worker punches in to or out of a time clock for another (absent) worker.

45. By marketing its biometric-enabled POS system in this manner, NCR obtains a competitive advantage over other POS systems, time and attendance solutions, and biometric verification companies and secures profits from its use of biometric data, all while failing to comply with the minimum requirements for handling workers' biometric data established by BIPA.

46. The Pay by Touch bankruptcy that catalyzed the passage of BIPA, as well as the recent data breaches, highlight why such conduct – where workers are aware that they are

providing a fingerprint but not aware to whom or for what purposes they are doing so – is dangerous. That bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers who exactly is collecting or obtaining their biometric data, where it will be transmitted and for what purposes, and for how long. Defendant disregards these obligations and workers' statutory rights and instead unlawfully collects, obtains, stores, uses and disseminates their biometric identifiers and information, without ever receiving the worker's informed written consent as required by BIPA.

47. Remarkably, NCR has created the same situation that Pay by Touch did by assembling a database of biometric data through broadly deployed biometric data readers and integrated, cloud-based software platforms, but failed to comply with the law specifically designed to protect workers whose biometrics are collected in these circumstances. Defendant disregards these obligations and Illinois workers' statutory rights and instead unlawfully collects, captures, obtains, stores, uses, and disseminates workers' biometric identifiers and information without ever receiving the worker's informed written consent, as required by BIPA.

48. Workers enrolled with NCR's biometric-enabled POS terminals and software (or who have their biometric data maintained or stored by NCR) are not told what might happen to their biometric data if and when NCR merges with another company, or worse, if and when NCR's business folds, or when the other third parties that have received their biometric data businesses fold.

49. Since Defendant did not first publish a BIPA-mandated data retention policy nor properly disclose the purposes for its collection, obtainment, and use of biometric data prior to its collection of biometric data, Plaintiffs and other similarly-situated workers enrolled with Defendant's biometric timekeeping devices and software have no idea whether Defendant sells,

discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiffs and others similarly situated are not told whom Defendant currently disclose their biometric data to, or what might happen to their biometric data in the event of a merger or a bankruptcy.

50. These violations have raised a material risk that Plaintiffs' and other similarly-situated workers' biometric data will be unlawfully accessed by third parties.

51. By and through the actions detailed above, Defendant disregards Plaintiffs' and other similarly-situated individuals' legal rights in violation of BIPA.

## III. Plaintiffs' Experience.

52. Plaintiff Michele Johnson worked as a Cook for Wingstop from October 2019 through November 2019 at its restaurant located at 2410 W. Jefferson Street, Joliet, Illinois 60435.

53. Plaintiff Christina Skeldon worked as a Cashier/Night Shift Lead for Wingstop from November 2017 through June 2020 at its restaurant located at 2410 W. Jefferson Street, Joliet, Illinois 60435.

54. Plaintiffs were required to scan their fingerprints at a biometric-enabled NCR POS system to be used as an authentication method to track their time worked and to access the POS terminal.

55. Specifically, Plaintiffs were required to scan and enroll their fingerprints with Wingstop's NCR database at Wingstop's biometric-enabled NCR POS system. NCR collected and/or otherwise obtained Plaintiffs' biometric data upon Plaintiffs' enrollment at Wingstop's biometric-enabled NCR POS system.

56. Plaintiffs were required to scan their fingerprints at Wingstop's biometric-enabled NCR POS system each time they accessed the POS terminal, including to clock in and out of work.

57. NCR subsequently collected and stored Plaintiffs' biometric data in NCR's cloud-based database(s), maintained on NCR's hosted environments and servers, each time they scanned their fingerprints to clock-in or clock-out or otherwise access the biometric-enabled NCR POS system.

58. NCR did not obtain Plaintiffs' consent before disclosing or disseminating their biometric data to third parties.

59. NCR did not properly inform Plaintiffs in writing of the specific limited purpose(s) or length of time for which their fingerprint data was being collected, obtained, stored, used and/or disseminated.

60. Plaintiffs had never seen, been able to access, or been informed of any publicly available biometric data retention policy or guidelines developed by Defendant, nor had they ever seen, been able to access, or been informed of whether Defendant would ever permanently delete their biometric data.

61. Plaintiffs have never been provided with, nor ever signed, a written release allowing NCR to collect, capture, obtain, store, use, and/or disseminate their biometric data.

62. Plaintiffs have continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's multiple violations of BIPA alleged herein.

63. No amount of time or money can compensate Plaintiffs if their biometric data is or has been compromised by the lax procedures through which NCR collects, captures, obtains, stores, disseminates, and/or uses Plaintiffs' and other similarly-situated workers' biometrics. Moreover, Plaintiffs would not have provided their biometric data to Defendant if they had known that Defendant would retain such information for an indefinite period of time without their consent.

64. 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").

65. As Plaintiffs are not required to allege or prove actual damages in order to state a claim under BIPA, they seek statutory damages under BIPA as compensation for the injuries caused by Defendant. *Rosenbach*, 2019 IL 123186, ¶ 40.

## CLASS ALLEGATIONS

66. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS § 5/2-801, Plaintiffs bring claims on their own behalf and as representatives 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.

67. 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, obtained, 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, obtained, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information. 740 ILCS § 14/15.

68. Plaintiffs seek 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 biometric identifier(s) and/or biometric information collected, captured, taken, received, converted, or otherwise obtained, maintained, stored, used, shared, disseminated, or disclosed by NCR during the applicable statutory period.

69. This action is properly maintained as a class action under 735 ILCS § 5/2-801 because:

A. The class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the class;

C. The claims of the Plaintiffs are typical of the claims of the class; and

D. The Plaintiffs will fairly and adequately protect the interests of the class.

**Numerosity**

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

**Commonality**

71. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiffs and all members of the Class have been harmed by Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether Defendant collected, captured, or otherwise obtained Plaintiffs' and the Class members' biometric identifiers or biometric information;

B. Whether Defendant properly informed Plaintiffs and the Class members of its purposes for collecting, obtaining, using, storing, and disseminating their biometric identifiers or biometric information;

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

D. Whether Defendant has disclosed or re-disclosed Plaintiffs' and the Class members' biometric identifiers or biometric information;

E. Whether Defendant has sold, leased, traded, or otherwise profited from Plaintiffs' and the Class members' biometric identifiers or biometric information;

F. Whether 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 Defendant used Plaintiffs' and the Class members' biometric identifiers to identify them;

H. Whether Defendant's violations of BIPA have raised a material risk that Plaintiffs' and the putative Class members' biometric identifiers and/or biometric information will be unlawfully accessed by third parties;

I. Whether Defendant's violations of BIPA were committed negligently; and

J. Whether Defendant's violations of BIPA were committed intentionally and/or recklessly.

72. Plaintiffs anticipate that Defendant will raise defenses that are common to the class.

**Adequacy**

73. Plaintiffs will fairly and adequately protect the interests of all members of the Class, and there are no known conflicts of interest between Plaintiffs and the Class members. Plaintiffs, moreover, have retained experienced counsel who are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

**Typicality**

74. The claims asserted by Plaintiffs are typical of the Class they seek to represent. Plaintiffs have the same interests and suffer from the same unlawful practices as the Class members.

75. 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**

76. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

77. 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 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**

78. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

79. 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).

80. Defendant failed to comply with these BIPA mandates.

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

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

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

84. Defendant failed to provide any publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

85. Defendant lacked retention schedules and guidelines for permanently destroying Plaintiffs' and the Class members' biometric data and did not destroy Plaintiffs' and the Class's

biometric data when the initial purpose for collecting or obtaining such data had been satisfied within three years of the individual's last interaction with the company.

86. On behalf of herself and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with BIPA's requirements for the collection, obtainment, 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**

87. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

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

89. Defendant failed to comply with these BIPA mandates.

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

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

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

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

94. Defendant did not properly inform Plaintiffs and the Class members in writing that their biometric identifiers and/or biometric information were being collected, obtained, stored, used, and disseminated, nor did Defendant properly inform Plaintiffs and the Class members in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being collected, obtained, stored, used, and disseminated as required by 740 ILCS § 14/15(b)(1)-(2).

95. By collecting, obtaining, storing, using, and disseminating Plaintiffs' and Class members' biometric identifiers and biometric information as described herein, Defendant violated Plaintiffs' and the Class's rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

96. On behalf of herself and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with BIPA's requirements for the collection, obtainment, storage,

use, and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

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

97. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

98. BIPA prohibits private entities from disclosing a person's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

99. Defendant fails to comply with this BIPA mandate.

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

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

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

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

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

105. On behalf of herself and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with BIPA's requirements for the collection, obtainment, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

**PRAYER FOR RELIEF**

Wherefore, Plaintiffs Michele Johnson and Christina Skeldon respectfully request that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs Michele Johnson and Christina Skeldon as Class Representatives, and appointing Stephan Zouras, LLP, as Class Counsel;

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

C. Awarding statutory damages of $5,000 for *each* intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS § 14/20(1);

D. Declaring that Defendant's actions, as set forth above, were intentional or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class, including an Order requiring Defendant to comply with BIPA when possessing, collecting, obtaining, storing, using,

destroying, and/or disseminating biometric identifiers and/or biometric information;

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

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

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

Date: May 4, 2022

Respectfully Submitted,

*/s/ Paige L. Smith*

Ryan F. Stephan
James B. Zouras
Anna M. Ceragioli
Paige L. Smith
**STEPHAN ZOURAS, LLP**
100 N. Riverside Plaza
Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com
jzouras@stephanzouras.com
aceragioli@stephanzouras.com
psmith@stephanzouras.com
Firm ID: 43734

**ATTORNEYS FOR PLAINTIFFS**

**CERTIFICATE OF SERVICE**

I, the attorney, hereby certify that on May 4, 2022, I electronically filed the attached with the Clerk of the Court using the electronic filing system and will send such filing to all attorneys of record.

*/s/ Paige L. Smith*