UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF ILLINOIS

MADISYN STAUFFER, on behalf of herself and all others similarly situated, Plaintiff, v. INNOVATIVE HEIGHTS FAIRVIEW HEIGHTS, LLC and PATHFINDER SOFTWARE, LLC, d/b/a CENTEREDGE SOFTWARE, LLC and SKY ZONE FRANCHISE GROUP, LLC Defendants.	)	Cause No. 3:20-cv-00046-MAB JURY TRIAL DEMANDED

THIRD AMENDED COMPLAINT

TABLE OF CONTENTS

Plaintiff Madisyn Stauffer, for her Third Amended Class Action Complaint ("Third Amended Complaint") against Defendants Innovative Heights Fairview Heights, LLC ("Innovative Heights"), Pathfinder Software, LLC, d/b/a CenterEdge Software, LLC ("CenterEdge"), and Sky Zone Franchise Group, LLC ("SZFG") alleges upon personal knowledge as to her own acts, and upon information and belief (based on the investigation of counsel) as follows[1]:

NATURE OF THE ACTION

1. This action involves Illinois' Biometric Information Privacy Act, 740 ILCS 14/1 *et seq*. ("BIPA"), a law that regulates companies' collection, use, safeguarding, handling, storage, retention, and destruction of biometric data.

2. Plaintiff was an employee of Innovative Heights at its Sky Zone facility located at 10850 Lincoln Trail, Fairview Heights, IL 62208 ("Sky Zone Fairview Heights"), who, along with other employees, scanned her fingerprints into CenterEdge's system to, *inter alia*, clock in or out of a shift and to log in to the computer system throughout the day, such as in connection with her use of the cash registry or after the system had "timed-out."

3. As set forth herein, each time Plaintiff scanned her fingerprint with the CenterEdge system, three separate entities—CenterEdge, SZFG, and Innovative Heights—collected, captured, purchased, received through trade, or otherwise obtained her biometric data.

4. None of the entities complied with the informed consent regime required by BIPA §15.

5. Plaintiff brings this action individually and on behalf of three separate Classes of similarly situated individuals whose biometric identifiers and/or biometric information was

[1] This Third Amended Complaint is filed pursuant to the Court's Orders dated August 5, 2022 and September 1, 2022.

possessed, collected, captured, purchased, received through trade, or otherwise obtained by CenterEdge (the "CenterEdge Class"), by SZFG (the "SZFG Class"), and by Innovative Heights (the "Innovative Heights Class"), in violation of BIPA.

6. CenterEdge is a technology company that provides hardware and software (the "CenterEdge System") to companies throughout Illinois, with a focus on companies with entertainment centers, amusement parks, waterparks, and trampoline parks.

7. To use the CenterEdge System, CenterEdge provides companies with a limited, non-exclusive license to use the CenterEdge software, typically for a one-year term, and sometimes also sells computer hardware with the software lease.

8. The CenterEdge software includes fingerprint matching/identification technology.

9. When a person's fingerprint is scanned with the CenterEdge System, CenterEdge scans, captures, collects, and stores in an electronic database digital copies of such fingerprints (the "biometric identifier").

10. When a person's fingerprint is scanned with the CenterEdge System, CenterEdge also creates additional information based on an individual's fingerprint that it uses to identify an individual. This additional information includes reference templates, algorithmic representations and/or codes based on the fingerprint that links the fingerprint to the individual (the "biometric information"). The biometric identifier and biometric information are collectively referred to herein as the "Biometric Data."

11. CenterEdge indefinitely stores and holds at its disposal the Biometric Data of its clients' employees in its electronic database in the CenterEdge System.

12. Each time a person's fingerprint is scanned with the CenterEdge System, CenterEdge collects, captures, receives, and/or obtains the Biometric Data and compares the

person's Biometric Data with associated Biometric Data previously stored in the CenterEdge database in order to identify an individual.

13. CenterEdge also controls and/or runs the systems and/or databases in which its clients' employees' Biometric Data is stored and/or receives the Biometric Data contained therein.

14. SZFG is the franchisor of several Sky Zone Indoor Trampoline Parks located in Illinois (the "Illinois Franchisees").

15. SZFG grants a license to the Illinois Franchisees to operate a Sky Zone Indoor Trampoline Park in accordance with the SZFG System and Intellectual Property.

16. The SZFG System "includes a unique, specially developed method of operating a Sky Zone Indoor Trampoline Park using the Intellectual Property, as well as selling other services (such as food, beverages, and parties) and products (including merchandise bearing the Marks), using certain procedures and methods, site evaluation criteria, layouts, advertising, sales and promotional techniques, personnel training, trade secrets and any other matters relating to the operation and promotion of a Sky Zone Indoor Trampoline Park, as they may be periodically changed, improved, modified and further developed by [SZFG] or [its] affiliates."

17. SZFG required its Illinois Franchisees, including Plaintiff's employer, Innovative Heights, to utilize the CenterEdge System, consisting of, *inter alia*, point-of-sale ("POS") computers and a limited, non-exclusive license to use the CenterEdge software.

18. The CenterEdge System that SZFG required to be used included CenterEdge's fingerprint matching/identification technology and software described above.

19. SZFG uses the CenterEdge System to collect, capture, receive, and/or obtain Biometric Data, which SZFG owns, controls, and holds at its disposal, to create reference

templates, algorithmic representations and/or codes based on its franchisees' employees' fingerprints that are linked to the fingerprint of the employee in order to, *inter alia*, prevent fraud, misconduct, or mismanagement by franchisee employees and to help ensure accurate royalty payments.

20. SZFG has taken numerous steps to acquire and own the Biometric Data of its Illinois Franchisees' employees.

21. In the franchise agreements, SZFG reserves to itself all rights not specifically granted to the franchisee. The franchise agreements do not grant the Illinois Franchisees any ownership rights over the data in the CenterEdge System.

22. Moreover, the Illinois Franchisees' access to the Biometric Data of their employees is restricted.

23. For example, Innovative Heights has explained in verified discovery responses that "the CenterEdge software does not give franchisees access to the fingerprint records."

24. CenterEdge's license agreements with SZFG's Illinois Franchisees also provide that CenterEdge "shall" share with and/or provide access to SZFG "all data stored in any CenterEdge system," which includes the Biometric Data.

25. SZFG's franchise agreements further explain that SZFG has the unlimited right to access and use the Biometric Data in the CenterEdge System at any time and for any purpose.

26. SZFG also can direct, and upon information and belief has directed, CenterEdge to remotely access the CenterEdge System of its franchisees.

27. SZFG can also independently access, modify, or delete the Biometric Data in the CenterEdge system remotely, and, upon information and belief, it remotely accesses the

CenterEdge Systems of its Illinois Franchisees using, *inter alia*, an application called TeamViewer, *which does not require CenterEdge's involvement*.

28. SZFG also requires that its franchisees "do all things necessary to give [SZFG] unrestricted access to the Technology System [which includes the CenterEdge System] at all times (including users IDs and passwords, if necessary) so that [SZFG] may independently download and transfer data via a modem or other connection that [SZFG] specif[ies]."

29. In addition to restricting franchisees' access to the Biometric Data and remotely accessing the data in the CenterEdge System, SZFG also regularly conducts in-person inspections of the CenterEdge System at the locations of its Illinois Franchisees. SZFG performs these inspections periodically via an SZFG "field consultant from the corporate office."

30. Upon information and belief, SZFG accessed the Biometric Data (a) remotely via the sharing and/or providing of information by CenterEdge; (b) remotely without CenterEdge via a TeamViewer or similar application in which SZFG "takes over," remotely accesses, and/or controls its franchisees' computers; (c) remotely without CenterEdge via an independent download or transfer of data from the CenterEdge System; and/or (d) in-person during a field consultant inspection of the CenterEdge System.

31. Further, SZFG expressly clarifies that SZFG, not the Illinois Franchisees, is the exclusive owner of the Biometric Data when it states in its franchise agreements that "[a]ll data pertaining to [a franchisee's] Business, and all data [a franchisee] create[s] or collect[s] . . . in connection with [its] operation of the Business . . . is and will be owned exclusively by [SZFG], and we will have the right to use such data in any manner that we deem appropriate without compensation to [the franchisee]."

32. Therefore, SZFG required its franchisees to furnish "all records of or relating to [the franchisee's] business," at any time if SZFG, in its sole discretion, requested. Likewise, when a franchise agreement with an Illinois Franchisee is terminated, the Illinois Franchisee must turn over all of its computer data to SZFG if SZFG, in its sole discretion, requests it.

33. Thus, in addition to requiring its Illinois Franchisees to use the CenterEdge system, SZFG has taken numerous steps to obtain and control the Biometric Data, including, but not limited to, by being the exclusive owner of the data. As the owner of the Biometric Data, SZFG has acquired the Biometric Data and holds it in its control and at its disposal.

34. Because of the manner in which the Biometric Data is collected, captured, handled, stored, and controlled, the Biometric Data of the employees of (a) CenterEdge's clients (b) the Illinois Franchisees, and (c) Innovative Heights is exposed to use and misuse by employees or agents of CenterEdge, SZFG, *or* Innovative Heights as well as compromise by a data breach or hack of CenterEdge, SZFG, *or* Innovative Heights.

35. Accordingly, CenterEdge, SZFG, and Innovative Heights are each private entities that have collected, captured, purchased, received through trade, or otherwise obtained Plaintiff's and the Class Members' biometric identifiers or biometric information.

36. CenterEdge, SZFG, and Innovative Heights, have each violated Plaintiff and the Class Members' rights under BIPA on numerous occasions by, *inter alia*:

- not properly informing Plaintiff and Class Members in writing that a biometric identifier and/or biometric information was being collected or stored as required by 740 ILCS 14/15(b)(1);
- not informing Plaintiff and Class Members in writing of the specific purpose and length of term for which a biometric identifier and/or biometric information was being collected, stored, or used as required by 740 ILCS 14/15(b)(2); and
- collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a biometric identifier and/or biometric information without

first obtaining the written release executed by Plaintiff and Class Members required by 740 ILCS 14/15(b)(3).

37. Additionally, CenterEdge and SZFG have each violated Plaintiff and the Class Members' rights under BIPA on numerous occasions by not developing, making available, and/or complying with a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and/or biometric information, and unlawfully retaining the biometric identifiers and/or biometric information of Plaintiff and Class Members, in violation of 740 ILCS 14/15(a).

38. As a result of Defendants' violations of BIPA, Plaintiff and the Class Members seek to recovery statutory and other damages and relief allowed under BIPA from each Defendant for each violation.

PARTIES

39. Plaintiff Madisyn Stauffer is a resident of Madison County, Illinois. She was employed by Innovative Heights and worked at the Sky Zone Fairview Heights facility from January of 2018 through May of 2018.

40. Defendant Innovative Heights is an Illinois Limited Liability Company, with its principal office located at 10850 Lincoln Trail, #12A, Fairview Heights, Illinois 62208. Its registered agent in Illinois is Bron Launsby, 10850 Lincoln Trail, #12A, Fairview Heights, Illinois 62208.

41. Innovative Heights owns Sky Zone Fairview Heights, a recreational facility/trampoline park that markets, advertises, and offers certain attractions and programs to the public, including attractions it describes as Freestyle Jump, SkySlam, Ultimate Dodgeball, SkyHoops, SkyJoust, SkyLadder, Warped Wall, FreeClimb, Foam Zone, Ninja Warrior Course, Laser Tag, and Drop Zone.

42. Innovative Heights conducts business in St. Clair County, Illinois, and transactions and conduct giving rise to the claims set forth in this Third Amended Complaint occurred in St. Clair County, Illinois. Specifically, Innovative Heights was the employer of Plaintiff and members of the Innovative Heights Class during all times that they worked at Sky Zone Fairview Heights, and the location of Sky Zone Fairview Heights where Plaintiff and Innovative Heights Class Members worked is in St. Clair County, Illinois.

43. Defendant CenterEdge is a North Carolina Limited Liability Company, with its principal office located at 5050 Durham Rd., Roxboro, NC 27574. Its registered agent in North Carolina is Robert E. Levin, 3511 Shannon Rd., Ste 140, Durham, NC 27707.

44. CenterEdge conducts business in St. Clair County, Illinois, and transactions and conduct giving rise to the claims set forth in this Third Amended Complaint occurred in St. Clair County, Illinois. Specifically, the location of Sky Zone Fairview Heights, with whom CenterEdge did business at its facility, is in St. Clair County, Illinois.

45. Defendant SZFG is a Missouri Limited Liability Company, with its principal office located at 1201 W. 5th Street, T-900, Los Angeles, CA 90017. Its registered agent in Missouri is Cogency Global Inc., 9666 Olive Boulevard, Suite 690, St. Louis, MO 63132.

46. SZFG conducts business in Illinois, and the transactions and conduct giving rise to the claims set forth in this Third Amended Complaint occurred in Illinois. Specifically, the locations of Innovative Heights and its other Illinois Franchisees, with whom SZFG did business at their facilities, are in Illinois.

JURISDICTION AND VENUE

47. This is a class action under Rule 23 of the Federal Rules of Civil Procedure.

48. This case was originally filed in the Circuit Court for St. Clair County, Illinois. Defendant CenterEdge removed this action to this Court pursuant to the Class Action Fairness Act, 18 U.S.C. § 1332(d) ("CAFA").

49. This Court has personal jurisdiction over Innovative Heights because it has its principal place of business in Illinois and, therefore, is a citizen of Illinois.

50. This Court has personal jurisdiction over all Defendants because they each purposefully direct their activities at residents of Illinois and the litigation arises out of or relates to those activities.

51. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 and §1441.

JURY DEMAND

52. For each Count in this Complaint, Plaintiff demands a jury trial to the extent it is allowed by law.

THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT

53. The Illinois General Assembly enacted BIPA in 2008 to establish regulations and standards of conduct for private entities related to biometric identifiers and biometric information.

54. Under BIPA, a "biometric identifier" includes an individual's fingerprints, and the term "biometric information" "means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10.

55. The Illinois General Assembly found that the use of biometrics has been growing, and "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information" in that unlike social security numbers or other identifiers that can be

changed when compromised, biometrics are "biologically unique to the individual; therefore, once compromised, the individual has no recourse . . . ." 740 ILCS 14/5(a)-(c).

56. BIPA is not limited to regulating the viewing, accessing, or use of biometric information. Instead, the Illinois General Assembly explained that BIPA "regulat[es] the collection, use, safeguarding, handling, storage, retention, and destruction" of biometric data. 740 ILCS 14/5(g).

57. Ultimately, BIPA "vests in individuals and customers the right to control their biometric information." *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 34 (Ill. 2019).

58. BIPA § 15(b) provides that a private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" unless it first informs that person in writing that such an identifier or information is being collected or stored; informs that person 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 receives a written release executed by the person who is the subject of the biometric identifier or information. 740 ILCS/14/15(b)(1)-(3).

59. The statute defines "written release" as "informed written consent or, in the context of employment, a release executed by an employee as a condition of employment." 740 ILCS 14/10.

60. BIPA § 15(a) requires that each "private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the

private entity, whichever occurs first." 740 ILCS 14/15(a). Additionally, "[a]bsent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines." *Id.*

61. Section 15(a) and 15(b) of BIPA do not require a private entity to ***have accessed or viewed*** biometric data to be subject to its regulations. In fact, the terms "access" and "view" do not appear in BIPA §15 (a), (b), (c), (d) or (e).[2] Moreover, one can possess or obtain data before accessing or viewing it.

62. "As the Illinois Supreme Court recognized in Rosenbach, the informed-consent regime laid out in section 15(b) is the heart of BIPA." *Bryant v. Compass Group USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020). "The text of the statute demonstrates that its purpose is to ensure that consumers understand, before providing their biometric data, how that information will be used, who will have access to it, and for how long it will be retained." *Id.*

63. Thus, § 15(b) is intended to provide people informed consent about to whom they will relinquish control over their biometric data. *Cothron v. White Castle Sys.*, 20 F.4th 1156, 1161 (7th Cir. 2021) ("[T]he duties imposed by section 15(b) reflect the General Assembly's judgment that people must have 'the opportunity to make informed choices about to whom and for what purpose they will relinquish control' over their biometric data.") (quoting *Bryant*, 958 F.3d at 626).

64. Finally, each different private entity that possesses, collects, captures, purchases, receives through trade, or otherwise obtains a person's biometric data must comply with § 15(a)

[2] The word "access" appears only once in BIPA, in an unrelated context as part of § 5(c), which states that "[b]iometrics are unlike other unique identifiers that are used to access finances or sensitive information." 740 ILCS 14/5(c).

and (b). "BIPA creates a scenario where each entity's violation gives rise to a claim; a plaintiff does not incur one, indivisible injury (e.g., a broken leg or lost cargo) caused by multiple defendants, but many individual injuries at the hands of many individual defendants who violated BIPA. And each entity is liable for its own violations, 'even if such violations occurred simultaneously or through use of the same equipment' as the violations of another entity." *Boyd v. Lazer Spot, Inc.*, No. 19 C 8173, 2022 U.S. Dist. LEXIS 131241, *2-3 (N.D. Ill. July 20, 2022) (quoting *Figueroa v. Kronos Inc.*, 454 F. Supp. 3d 772, 787 (N.D. Ill. 2020)).

65. Therefore, each private entity to whom a person relinquishes control of his or her biometric data puts the person's biometric data, which is "immutable, and once compromised, [is] compromised forever," at "risk of identity theft or other privacy or economic harm" where "the individual has no recourse." *Fox v. Dakkota Intergrated Sys., LLC*, 980 F.3d 1146, 1155 (7th Cir. 2020); *Bryant*, 958 F.3d at 626; 740 ILCS 14/5(c).

FACTUAL ALLEGATIONS

Plaintiff's Experience

66. Plaintiff began her employment with Innovative Heights in January of 2018 and worked for Innovative Heights as a Cashier, Event Host, and Event Planner at its Sky Zone Fairview Heights facility.

67. When Plaintiff began her employment with Innovative Heights, she was required to scan her fingerprints into the CenterEdge System.

68. CenterEdge created additional biometric information derived from Plaintiff's fingerprints that was used to identify Plaintiff.

69. Plaintiff's fingerprint and the biometric information created by CenterEdge (collectively "Plaintiff's Biometric Data") was thereafter stored in the CenterEdge System.

70. Plaintiff's Biometric Data was used in lieu of a more traditional time clock, in that she scanned her fingerprints into the CenterEdge system each time she "clocked in" or "clocked out" of work throughout her employment with Innovative Heights.

71. Plaintiff also scanned her fingerprints at additional times throughout her employment in connection with her use of the cash register. Specifically, if she had not recently been helping a customer and the cash register had timed out and needed to be "woken up," she had to do so by scanning her fingerprints into the CenterEdge System.

72. Thus, Plaintiff and other Class Members using the CenterEdge System scanned their fingerprints multiple times during the workday.

73. Plaintiff's employment with Innovative Heights ended in mid-2018.

CenterEdge Violated BIPA

74. When a person initially scans his/her fingerprint into the CenterEdge System, CenterEdge captures, collects, creates, and stores in its database a digital image of the fingerprint. This digital fingerprint is a "biometric identifier" under BIPA.

75. From this fingerprint image, CenterEdge then extracts unique characteristics and creates additional data, commonly known as Fingerprint Minutiae Data, which is used to identify an individual.

76. This additional information created by CenterEdge includes reference templates, algorithmic representations and/or codes based on the fingerprint that links the fingerprint to the individual, and constitutes "biometric information" under BIPA.

77. CenterEdge sometimes refers to the additional information it creates from the fingerprint image as "a string of data known as a 'hash.'"

78. Thus, CenterEdge collects, captures, creates, receives, or otherwise obtains, biometric identifiers and biometric information.

79. CenterEdge also stores the biometric identifiers and biometric information on its database in the CenterEdge System and, therefore, collects, captures, purchases, receives through trade, or otherwise obtains the biometric data.

80. CenterEdge's website explains that as a "leader in the entertainment software industry," it "operate[s] as a processor of personal information for our customer . . . ."

81. CenterEdge's website goes on to say that information collected by its clients with the CenterEdge System will be considered as being provided to CenterEdge.[3]

82. CenterEdge also controls and/or runs the systems and/or databases in which its clients' employees' Biometric Data is stored, and indefinitely stores and holds at its disposal in an electronic database digital copies of its clients' employees' Biometric Data.

83. One CenterEdge client has explained in responding to a subpoena by Plaintiff that CenterEdge "hosts Employee data for [the CenterEdge client]" and that "[a]utomated CenterEdge backups of active [client] databases occur on an incremental daily and weekly basis."

84. According to the CenterEdge license agreements, CenterEdge clients are only allowed to store "*copies* of the data of Customer resulting from the use by Customer of the Software."

85. Moreover, according to Innovative Heights' verified interrogatory responses, "the CenterEdge software does not give franchisees access to the fingerprint records."

86. Additionally, when Plaintiff requested information about the fingerprint data in subpoenas served on CenterEdge's clients in this case, two clients, who are also SZFG

[3] *See* "Advantage Access Control," available at https://centeredgesoftware.com/advantage-access-control/ (accessed 8/12/22).

franchisees, explained they did not have access to the information in the CenterEdge System to respond to the subpoena "due to an unexpected cessation of service by CenterEdge."

87. According to CenterEdge, this cessation of service occurred when these franchisees "stopped paying for services, claim[ed] that they have terminated services but never followed the process to do so, and [CenterEdge] is currently suing them for the past due balance."

88. Thus, if CenterEdge's license agreement ends, the Biometric Data is not automatically deleted, the former CenterEdge client can no longer access or use the CenterEdge System, yet CenterEdge continues to control and hold the data at its disposal.

89. Accordingly, each time Plaintiff and the CenterEdge Class Members had their fingerprint scanned with a CenterEdge System, CenterEdge collected, captured, purchased, received through trade, or otherwise obtained their biometric identifiers and/or biometric information.

90. As set forth herein, CenterEdge was also in possession of the biometric identifiers and/or biometric information of Plaintiff and the CenterEdge Class.

91. As an entity creating Biometric Data, controlling that data, and holding it at its disposal, CenterEdge is responsible for safeguarding, handling, storing, retaining, and destroying that data.

92. Because of the manner in which the Biometric Data is collected, captured, handled, stored, and controlled, the Biometric Data of the employees of CenterEdge's clients is exposed to use or misuse by CenterEdge's employees and agents as well as compromise by a data breach or hack of CenterEdge.

93. CenterEdge failed to inform Plaintiff and the CenterEdge Class Members in writing that a biometric identifier and/or biometric information was being collected or stored.

94. CenterEdge also failed to inform Plaintiff and the CenterEdge Class Members in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used.

95. CenterEdge also failed to obtain a written release from Plaintiff and the CenterEdge Class Members before collecting, capturing, purchasing, receiving through trade, or otherwise obtaining biometric identifiers and/or biometric information.

96. CenterEdge's actions have prevented Plaintiff and the CenterEdge Class Members from giving their informed consent and having access to important information to give them "the opportunity to make informed choices about to whom and for what purpose they will relinquish control over their biometric data." *Cothron*, 20 F.4th at 1161 (internal quotation marks omitted).

97. In addition, CenterEdge, as an entity creating, controlling, and holding biometric data at its disposal, was responsible for retaining and deleting such data in compliance with the law.

98. CenterEdge did not develop, publicly disclose, and/or comply with a written policy establishing a retention schedule and guidelines for permanently destroying these biometric identifiers and biometric information to occur by the earlier of: (a) when the original purpose for collecting or obtaining such identifiers has been satisfied, or (b) within 3 years of the individual's last interaction with the private entity.

99. CenterEdge's failure to maintain and comply with a data retention and destruction policy harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the CenterEdge Class, including the right to make informed choices about the use of and control

over their inherently sensitive biometric data and to be free from unlawful retention of such sensitive data.

SZFG Violated BIPA

100. SZFG is the franchisor of the Illinois Franchisees, which includes Innovative Heights.

101. Each Illinois Franchisee must enter into a Franchise Agreement with SZFG (a "Franchise Agreement").

102. In the Franchise Agreements, SZFG grants the Illinois Franchisees limited rights, in the form of a license to operate a Sky Zone Indoor Trampoline Park in accordance with the SZFG System and Intellectual Property.

> **Grant of License.** Subject to the terms and conditions herein, SFG hereby grants to FRANCHISEE, and FRANCHISEE hereby accepts from SFG, a non-exclusive right to operate one, and only one, Sky Zone Indoor Trampoline Park to be located at the location listed in Exhibit I attached hereto ("Site") in accordance with the System and Intellectual Property.

103. The SZFG System "includes a unique, specially developed method of operating a Sky Zone Indoor Trampoline Park using the Intellectual Property," which includes "using certain procedures and methods, . . . personnel training, trade secrets and any other matters relating to the operation and promotion of a Sky Zone Indoor Trampoline Park, as they may be periodically changed, improved, modified and further developed by [SZFG] or [its] affiliates."

104. As part of the System of certain procedures, methods, and other matter relating to the operation of a Sky Zone Indoor Trampoline Park, SZFG required the Illinois Franchisees, including Innovative Heights, to utilize the CenterEdge System, consisting of, *inter alia*, point-of-sale ("POS") computer systems and a limited, non-exclusive license to use the CenterEdge software.

105. SZFG provides each Illinois Franchisee a "Franchise Disclosure Document" that describes in more detail the equipment required and SZFG's rights related to the equipment and data stored therein.

106. The Franchise Disclosure Documents states that the franchisee must use the computer system that SZFG requires and the CenterEdge software:

> You must use the computer system we require ("POS System"). You will need to enter into an agreement with CenterEdge Software, LLC to obtain the right to use the customized software they have developed for us and the cost of the installation.

107. SZFG also reserves its rights to modify or require different or additional software programs and hardware at any time:

> We [SZFG] may revise our specifications for hardware and software as we determine necessary to meet the needs of the System and there is no contractual limitation on our ability to require the hardware or software to be changed, improved or upgraded. We reserve the right to require different or additional software programs and hardware at any time in the future and you must pay for the cost of any new, modified or updated programs and the hardware. There is no limitation in the Franchise Agreement on either our right to require you to obtain updates or upgrades or the cost of any updates or upgrades.

108. SZFG also provided its Illinois Franchisees a breakdown of "required items" they must purchase from "required vendors." This breakdown included a category for "Computer Software License and Hardware," in which CenterEdge Software was listed as the vendor. The breakdown of items included: "Time Clock/Employee Scheduling Module"; and "All-in-one Workstation" that includes an "Integrated Magstripe + Fingerprint."

109. The CenterEdge System that SZFG required for the Illinois Franchisees also included CenterEdge's fingerprint matching/identification technology and software described above.

110. As set forth herein, SZFG used the CenterEdge System to collect, capture, receive, and/or obtain Biometric Data, which SZFG owns, controls, and holds at its disposal, to create reference templates, algorithmic representations and/or codes based on its franchisees' employees' fingerprints that are linked to the fingerprint of the employee in order to, *inter alia*, prevent fraud, misconduct, or mismanagement by franchisee employees and to help ensure accurate royalty payments.

111. In addition to requiring the Illinois Franchisees to use the CenterEdge System, SZFG took numerous steps to get, acquire, secure, control, and hold the Biometric Data at its disposal.

112. In the Franchise Agreements, SZFG reserves to itself all rights not specifically granted to the franchisee.

> **Rights Reserved.** SFG, on behalf of itself and its Affiliates, reserves all rights not specifically granted to the FRANCHISEE pursuant to this Agreement.

113. The Franchise Agreements do not grant the Illinois Franchisees any ownership rights over the data in the CenterEdge System. Thus, SZFG owns all such data.

114. SZFG's Franchise Agreements further explain that SZFG has complete control over all data in the CenterEdge System, including the unlimited right to independently access and use the Biometric Data in the CenterEdge system at any time and for any purpose:

> We will have the right to have independent access to all information or data in the POS System and the surveillance system, and there are no limitations on our rights to do so. We will also have the right to use and publish the information we collect from your POS System in our discretion, including disclosure in our Franchise Disclosure Document. We are not obligated to provide or to assist you in obtaining the above item or services. In the future, you may be required to change, upgrade or modify the type of computer hardware and software you must use at your expense.

115. SZFG gained access to the data in the CenterEdge System in various ways.

116. CenterEdge's license agreements with the Illinois Franchisees provided that CenterEdge "will" and "shall" share with and/or provide access to SZFG "all data stored in any CenterEdge system," which includes the Biometric Data:

> 6. **REMOTE ACCESS**
>
> Customer [franchisee] agrees to allow CenterEdge to share and/or provide access to information created as a result of this Agreement with Customer with the third parties listed in Exhibit D. This shared information includes, but is not limited to, all data stored in any CenterEdge system . . . .
>
> * * * *
>
> **Exhibit D**
>
> **Remote Access**
>
> CenterEdge will provide access to the following entities as set forth in Article 6:
>
> CenterEdge shall provide access, pursuant to Article 6 of the Agreement, to . . . Sky Zone Franchise Group, LLC . . . .

117. Thus, while, in the words of Innovative Heights, "the CenterEdge software does not give franchisees access to the fingerprint records," it does give SZFG unrestricted access to such data.

118. Upon information and belief, SZFG directed CenterEdge to add SZFG and its affiliates to Exhibit D of CenterEdge's license agreements with the Illinois Franchisees to, *inter alia*, exert and clarify its control over all the data in the CenterEdge Systems of the Illinois Franchisees.

119. In addition to having remote access to the Biometric Data via CenterEdge, SZFG could also *independently* access, modify, or delete the Biometric Data in the CenterEdge system

remotely, and it remotely accesses the CenterEdge Systems of its Illinois Franchisees using, *inter alia*, an application called TeamViewer, which does not require CenterEdge's involvement.

120. SZFG also required that its franchisees "do all things necessary to give [SZFG] unrestricted access to the Technology System [which includes the CenterEdge System] at all times (including users IDs and passwords, if necessary) so that [SZFG] may independently download and transfer data via a modem or other connection that [SZFG] specif[ies]."

121. In addition to remotely accessing the data in the CenterEdge System, SZFG also regularly, and periodically, conducted in-person inspections of all records in the CenterEdge System at the locations of its Illinois Franchisees.

122. SZFG performed these inspections periodically via an SZFG "field consultant from the corporate office."

123. Upon information and belief, SZFG accessed the Biometric Data (a) remotely via the sharing and/or providing of information by CenterEdge; (b) remotely without CenterEdge via a TeamViewer or similar application in which SZFG "takes over," remotely accesses, and/or controls its franchisees' computers; (c) remotely without CenterEdge via an independent download or transfer of data; and/or (d) in-person during a field consultant inspection.

124. SZFG also can direct, and upon information and belief has directed, CenterEdge to remotely access the CenterEdge System of its franchisees.

125. These steps by SZFG demonstrate that SZFG has complete control over, and owns, the Biometric Data in the CenterEdge Systems of its Illinois Franchisees.

126. SZFG's ownership of the Biometric Data is also further evidenced by the provisions of its Franchise Agreements and Operations Manual in which SZFG required its

franchisees to furnish "all records of or relating to [the franchisee's] business," at any time if SZFG, in its sole discretion, requested.

127. SZFG's ownership of the Biometric Data is further evidenced by the provision in its Franchise Agreements stating that, upon termination of a Franchise Agreement, the Illinois Franchisees must turn over all of its computer data to SZFG upon SZFG's request—that is, in the sole discretion of SZFG, which owns the data.

128. Furthermore, in or prior to 2018, SZFG took another step and clarified with franchisees that it "exclusively" owns the Biometric Data when it expressly stated in its franchise agreements that "[a]ll data pertaining to [a franchisee's] Business, and all data [a franchisee] create[s] or collect[s] . . . in connection with [its] operation of the Business . . . is and will be owned exclusively by [SZFG], and [SZFG] will have the right to use such data in any manner that [it] deem[s] appropriate without compensation to [the franchisee]."

> All data pertaining to your Business, and all data you create or collect in connection with the System, or in connection with your operation of the Business (including data pertaining to or otherwise concerning your members) or otherwise provided by you (including data uploaded to, or downloaded from your computer system) is and will be owned exclusively by us [SZFG], and we will have the right to use such data in any manner that we deem appropriate without compensation to you. Such data will be part of the Confidential Information. We hereby license use of such data back to you for the term of this Agreement, at no additional cost, solely for your use in connection with the Business conducted under this Agreement.

129. An entity that owns and controls data on a server that it can access at any time and for any reason has obtained that data, even if an employee of the entity has not viewed or accessed that data.

130. Moreover, SZFG, not the Illinois Franchisees, is the entity that has the right and ability to delete the Biometric Data.

131. As the owner and controller of the Biometric Data, SZFG is responsible for safeguarding, handling, storing, retaining, and destroying that data.

132. Because of the manner in which the Biometric Data is collected, captured, handled, stored, and controlled, the Biometric Data of the employees of SZFG's Illinois Franchisees is exposed to use or misuse by SZFG's employees and agents as well as compromise by a data breach or hack of SZFG.

133. SZFG, an entity that is the exclusive owner of data, with unlimited and unrestricted control over the data, with unfettered access to and use of the data, and which has limited the rights of others to that data, has taken active steps to get, acquire, secure, control, and hold the data at its disposal.

134. Accordingly, SZFG collected, captured, purchased, received through trade, or otherwise obtained the biometric identifiers and/or biometric information of Plaintiff and the SZFG Class Members.

135. As set forth herein, SZFG was also in possession of the biometric identifiers and/or biometric information of Plaintiff and the SZFG Class.

136. SZFG failed to inform Plaintiff and the SZFG Class Members in writing that a biometric identifier and/or biometric information was being collected or stored.

137. SZFG also failed to inform Plaintiff and the SZFG Class Members in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used.

138. SZFG also failed to obtain a written release from Plaintiff and the SZFG Class Members before collecting, capturing, purchasing, receiving through trade, or otherwise obtaining biometric identifiers and/or biometric information.

139. SZFG's actions have prevented Plaintiff and the SZFG Class Members from giving their informed consent and having access to important information to give them "the opportunity to make informed choices about to whom and for what purpose they will relinquish control over their biometric data." *Cothron*, 20 F.4th at 1161 (internal quotation marks omitted).

140. In addition, SZFG as an entity owning, controlling, and holding biometric data at its disposal, was responsible for retaining and deleting such data in compliance with the law.

141. SZFG did not develop, publicly disclose, and/or comply with a written policy establishing a retention schedule and guidelines for permanently destroying these biometric identifiers and biometric information to occur by the earlier of: (a) when the original purpose for collecting or obtaining such identifiers has been satisfied, or (b) within 3 years of the individual's last interaction with the private entity.

142. SZFG's failure to maintain and comply with a data retention and destruction policy harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the SZFG Class, including the right to make informed choices about the use of and control over their inherently sensitive biometric data and to be free from unlawful retention of such sensitive data.

Innovative Heights Violated BIPA

143. Innovative Heights also collected, captured, received through trade, or otherwise obtained Plaintiff's and Innovative Heights Class Members' biometric identifiers (fingerprints) at the beginning of their employment with Innovative Heights and each time thereafter when Plaintiff and Innovative Heights Class Members scanned their fingerprints to "clock in" or "clock out" or to awaken the cash register.

144. Innovative Heights also collected, captured, received through trade, or otherwise obtained the biometric information described above used to identify Plaintiff and the Innovative Heights Class Members.

145. Because of the manner in which the Biometric Data is collected, captured, handled, stored, and controlled, the Biometric Data of the employees of Innovative Heights is exposed to use or misuse by SZFG's employees and agents as well as compromise by a data breach or hack of Innovative Heights.

146. Innovative Heights failed to inform Plaintiff and the Innovative Heights Class Members in writing that a biometric identifier and/or biometric information was being collected or stored.

147. Innovative Heights also failed to inform Plaintiff and the Innovative Heights Class Members in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used.

148. Innovative Heights also failed to obtain a written release from Plaintiff and the Innovative Heights Class Members before collecting, capturing, receiving through trade, or otherwise obtaining biometric identifiers and/or biometric information

149. Innovative Heights' actions have prevented Plaintiff and the Innovative Heights Class Members from giving their informed consent and having access to important information to give them "the opportunity to make informed choices about to whom and for what purpose they will relinquish control over their biometric data." *Cothron*, 20 F.4th at 1161 (internal quotation marks omitted).

CLASS ACTION ALLEGATIONS

150. Plaintiff brings this action on behalf of three classes of similarly situated individuals whose rights under BIPA were violated by CenterEdge, SZFG, and Innovative Heights.

151. Specifically, Plaintiff seeks certification of the following Classes, defined as follows:

"CenterEdge Class"

All Illinois citizens who, during the Class Period, scanned one or more fingerprint into a CenterEdge System at a CenterEdge client located in Illinois prior to: (1) CenterEdge having a written policy made available to the public that established a retention schedule and guidelines for the destruction of such biometric identifiers or biometric information and/or (2) (a) receiving written information that a biometric identifier or biometric information was being collected or stored and the purpose and length thereof; and/or (b) providing a written release. Excluded from the CenterEdge Class is any person who has or had a controlling interest in CenterEdge.

"SZFG Class"

All Illinois citizens who, during the Class Period, scanned one or more fingerprint into a CenterEdge System at an Illinois Franchisee location prior to: (1) SZFG having a written policy made available to the public that established a retention schedule and guidelines for the destruction of such biometric identifiers or biometric information and/or (2) (a) receiving written information that a biometric identifier or biometric information was being collected or stored and the purpose and length thereof; and/or (b) providing a written release. Excluded from the SZFG Class is any person who has or had a controlling interest in SZFG.

"Innovative Heights Class"

All Illinois citizens who, during the Class Period, scanned one or more fingerprint into a CenterEdge System at the Innovative Heights location prior to: (1) receiving written information that a biometric identifier or biometric information was being collected or stored and the purpose and length thereof; and/or (2) providing a written release. Excluded from the Innovative Heights Class is any person who has or had a controlling interest in Innovative Heights.

Plaintiff may modify these class definitions based on discovery yet to be taken.

152. The Class Period is that period within the statute of limitations for this action and extending until a Class is certified herein.

153. Numerosity. The exact size of the Classes are currently unknown to Plaintiff, but on information and belief the total number of members in the Classes is, at a minimum, in the thousands, and the Classes are so numerous that joinder of all Class Members would be impracticable.

154. Commonality. There is a well-defined community of interest in the questions of law and fact affecting the members of the Classes, and questions of law and fact common to the Classes predominate over any questions affecting only individual members. Among the numerous questions of law or fact common to the CenterEdge Class are the following:

a. Whether CenterEdge was in possession of biometric identifiers and/or biometric information;

b. Whether CenterEdge collected, captured, purchased, received through trade, or otherwise obtained Plaintiff's and CenterEdge Class Members' biometric identifiers or biometric information;

c. Whether CenterEdge informed Plaintiff and CenterEdge Class Members in writing that a biometric identifier or biometric information was being collected or stored;

d. Whether CenterEdge informed Plaintiff and CenterEdge Class Members in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used;

e. Whether CenterEdge received written releases from Plaintiff and CenterEdge Class Members before capturing, collecting, purchasing, receiving through trade, or otherwise obtaining their biometric identifiers or biometric information;

f. Whether and when CenterEdge developed, made available to the public, and complied with a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and/or biometric information in accordance with BIPA §15(a); and

g. Whether any violations of BIPA by CenterEdge were negligent, or rather were reckless or intentional.

155. Among the numerous questions of law or fact common to the SZFG Class are the following:

a. Whether SZFG was in possession of biometric identifiers and/or biometric information;

b. Whether SZFG collected, captured, purchased, received through trade, or otherwise obtained Plaintiff's and SZFG Class Members' biometric identifiers or biometric information;

c. Whether SZFG informed Plaintiff and SZFG Class Members in writing that a biometric identifier or biometric information was being collected or stored;

d. Whether SZFG informed Plaintiff and SZFG Class Members in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used;

e. Whether SZFG received written releases from Plaintiff and SZFG Class Members before capturing, collecting, purchasing, receiving through trade, or otherwise obtaining their biometric identifiers or biometric information;

f. Whether and when SZFG developed, made available to the public, and complied with a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and/or biometric information in accordance with BIPA §15(a); and

g. Whether any violations of BIPA by SZFG were negligent, or rather were reckless or intentional.

156. Among the numerous questions of law or fact common to the Innovative Heights Class are the following:

a. Whether Innovative Heights collected, captured, received through trade, or otherwise obtained Plaintiff's and Innovative Heights Class Members' biometric identifiers or biometric information;

b. Whether Innovative Heights informed Plaintiff and Innovative Heights Class Members in writing that a biometric identifier or biometric information was being collected or stored;

c. Whether Innovative Heights informed Plaintiff and Innovative Heights Class Members in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used;

d. Whether Innovative Heights received written releases from Plaintiff and Innovative Heights Class Members before capturing, collecting, receiving through trade, or otherwise obtaining their biometric identifiers or biometric information; and

e. Whether any violations of BIPA by Innovative Heights were negligent, or rather were reckless or intentional.

157. Typicality. The claims of Plaintiff are typical of the claims of the members of the Classes. Plaintiff and all members of each Class have had their rights under BIPA violated based on each Defendant's failure to comply with the provisions of BIPA.

158. Adequacy of Representation. Plaintiff is an adequate representative of the Classes and has no conflict of interest with other members of the Classes. Plaintiff's attorneys are experienced in this type of litigation and will prosecute the action vigorously on behalf of the Classes.

159. Superiority. A class action is an appropriate method to adjudicate this controversy and is superior to any other available methods for the fair and efficient adjudication of this controversy. Plaintiff knows of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action. Furthermore, the prosecution of separate actions by individual members of the Classes would create a risk of inconsistent and varying adjudications concerning the subject of this action. A class action would conserve the resources of the courts and litigants and further efficient adjudication of the claims of the members of the Classes.

COUNT I: INNOVATIVE HEIGHTS' VIOLATION OF 740 ILCS 14/1, *et seq.*
(Plaintiff and the Innovative Heights Class)

160. Plaintiff realleges and incorporates by reference all preceding paragraphs of this Third Amended Complaint as though fully set forth herein.

161. The fingerprints of Plaintiff and the Innovative Heights Class Members constitute "biometric identifiers" pursuant to 740 ILCS 14/10.

162. All other information based on Plaintiff's and the Innovative Heights Class Members' fingerprints used to identify such class member constitutes "biometric information" pursuant to 740 ILCS 14/10.

163. As set forth herein, Innovative Heights violated Plaintiff's and Innovative Heights Class Members' rights under BIPA by collecting, capturing, receiving through trade, or otherwise obtaining their biometric identifiers and/or biometric information without first:

a. informing Plaintiff and Innovative Heights Class Members in writing that a biometric identifier or biometric information was being collected or stored;

b. informing Plaintiff and Innovative Heights Class Members in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used; and/or

c. receiving a written release executed by Plaintiff and Innovative Heights Class Members.

740 ILCS 14/15(b)(1)-(3).

164. Innovative Heights' failure to disclose its practices and obtain the informed consent of Plaintiff and the Innovative Heights Class Members before collecting, capturing, purchasing, receiving through trade, or otherwise obtaining their biometric data harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the Innovative Heights Class, including the right to make informed choices about the use of and control over their inherently sensitive biometric data.

165. Plaintiff's and Innovative Heights Class Members' rights under BIPA were violated by Innovative Height's failure to comply with BIPA as set forth above, and in so violating BIPA, Innovative Heights acted negligently, recklessly and/or intentionally.

166. Plaintiff and Innovative Heights Class Members are "aggrieved" under BIPA based on Innovative Heights' violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

167. Plaintiff and Innovative Heights Class Members are therefore entitled to damages available under BIPA, including liquidated damages of $1,000 for each and every negligent violation, or alternatively, $5,000 for each and every intentional or reckless violation, or actual damages, whichever is greater, injunctive relief, and further damages and relief as set forth in the PRAYER FOR RELIEF below. 740 ILCS 14/20(1)-(4).

COUNT II: CENTEREDGE'S VIOLATION OF 740 ILCS 14/1, *et seq.*
(Plaintiff and the CenterEdge Class)

168. Plaintiff realleges and incorporates by reference all preceding paragraphs of this Third Amended Complaint as though fully set forth herein.

169. The fingerprints of Plaintiff and the CenterEdge Class Members constitute "biometric identifiers" pursuant to 740 ILCS 14/10.

170. All other information based on Plaintiff's and the CenterEdge Class Members' fingerprints used to identify such class member constitutes "biometric information" pursuant to 740 ILCS 14/10.

171. As set forth herein, on numerous occasions during the Class Period, CenterEdge has been in possession of Plaintiff's and the CenterEdge Class Members' biometric identifiers and/or biometric information.

172. Prior to and while possessing Plaintiff's and the CenterEdge Class Members' biometric identifiers and/or biometric information, CenterEdge did not develop, publicly disclose, and/or comply with a written policy establishing a retention schedule and guidelines for permanently destroying these biometric identifiers and biometric information to occur by the earlier of: (a) when the original purpose for collecting or obtaining such identifiers has been satisfied, or (b) within 3 years of the individual's last interaction with the private entity, as required by 740 ILCS 14/15(a).

173. CenterEdge further failed to permanently destroy the biometric identifiers and/or biometric information of Plaintiff and the CenterEdge Class in the period required by BIPA §15(a).

174. CenterEdge's failure to maintain and comply with a biometric data retention and destruction policy, and its unlawful retention of the biometric identifiers and/or biometric information of Plaintiff and the CenterEdge Class Members harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the CenterEdge Class, including the right to make informed choices about the use of and control over their inherently sensitive biometric data and to be free from unlawful retention of such sensitive data.

175. CenterEdge violated Plaintiff's and CenterEdge Class Members' rights under BIPA by collecting, capturing, purchasing, receiving through trade, or otherwise obtaining their biometric identifiers and/or biometric information without first:

a. informing Plaintiff and CenterEdge Class Members in writing that a biometric identifier or biometric information was being collected or stored;

b. informing Plaintiff and CenterEdge Class Members in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used;

c. receiving a written release executed by Plaintiff and CenterEdge Class Members.

740 ILCS 14/15(b)(1)-(3).

176. CenterEdge's failure to disclose its practices and obtain the informed consent of Plaintiff and the CenterEdge Class Members before collecting, capturing, purchasing, receiving through trade, or otherwise obtaining their biometric data harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the CenterEdge Class, including the right to make informed choices about the use of and control over their inherently sensitive biometric data.

177. Plaintiff's and CenterEdge Class Members' rights under BIPA were violated by CenterEdge's failure to comply with BIPA as set forth above, and in so violating BIPA, CenterEdge acted negligently, recklessly and/or intentionally.

178. Plaintiff and CenterEdge Class Members are "aggrieved" under BIPA based on CenterEdge's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

179. Plaintiff and CenterEdge Class Members are therefore entitled to damages available under BIPA, including liquidated damages of $1,000 for each and every negligent violation, or alternatively, $5,000 for each and every intentional or reckless violation, or actual damages, whichever is greater, injunctive relief, and further damages and relief as set forth in the PRAYER FOR RELIEF below. 740 ILCS 14/20(1)-(4).

COUNT III: SZFG'S VIOLATION OF 740 ILCS 14/1, *et. seq.*
(Plaintiff and the SZFG Class)

180. Plaintiff realleges and incorporates by reference all preceding paragraphs of this Third Amended Complaint as though fully set forth herein.

181. The fingerprints of Plaintiff and the SZFG Class Members constitute "biometric identifiers" pursuant to 740 ILCS 14/10.

182. All other information based on Plaintiff's and the SZFG Class Members' fingerprints used to identify such class member constitutes "biometric information" pursuant to 740 ILCS 14/10.

183. As set forth herein, on numerous occasions during the Class Period, SZFG has been in possession of Plaintiff's and the SZFG Class Members' biometric identifiers and/or biometric information.

184. Prior to and while possessing Plaintiff's and the SZFG Class Members' biometric identifiers and/or biometric information, SZFG did not develop, publicly disclose, and/or comply with a written policy establishing a retention schedule and guidelines for permanently destroying these biometric identifiers and biometric information to occur by the earlier of: (a) when the original purpose for collecting or obtaining such identifiers has been satisfied, or (b) within 3 years of the individual's last interaction with the private entity, as required by 740 ILCS 14/15(a).

185. SZFG further failed to permanently destroy the biometric identifiers and/or biometric information of Plaintiff and the SZFG Class in the period required by BIPA §15(a).

186. SZFG's failure to maintain and comply with a biometric data retention and destruction policy, and its unlawful retention of the biometric identifiers and/or biometric information of Plaintiff and the SZFG Class Members harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the SZFG Class, including the right to make informed choices about the use of and control over their inherently sensitive biometric data and to be free from unlawful retention of such sensitive data.

187. SZFG violated Plaintiff's and SZFG Class Members' rights under BIPA by collecting, capturing, purchasing, receiving through trade, or otherwise obtaining their biometric identifiers and/or biometric information without first:

a. informing Plaintiff and SZFG Class Members in writing that a biometric identifier or biometric information was being collected or stored;

b. informing Plaintiff and SZFG Class Members in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being collected, stored, and used;

c. receiving a written release executed by Plaintiff and SZFG Class Members.

740 ILCS 14/15(b)(1)-(3).

188. SZFG's failure to disclose its practices and obtain the informed consent of Plaintiff and the SZFG Class Members before collecting, capturing, purchasing, receiving through trade, or otherwise obtaining their biometric data harmed, or posed a material risk of harm to, the concrete privacy interests of Plaintiff and the SZFG Class, including the right to make informed choices about the use of and control over their inherently sensitive biometric data.

189. Plaintiff's and SZFG Class Members' rights under BIPA were violated by SZFG's failure to comply with BIPA as set forth above, and in so violating BIPA, SZFG acted negligently, recklessly and/or intentionally.

190. Plaintiff and SZFG Class Members are "aggrieved" under BIPA based on SZFG's violation of their rights under BIPA, and accordingly are entitled to seek damages and relief provided for under the statute. *See Rosenbach*, 2019 IL 123186, ¶ 40.

191. Plaintiff and SZFG Class Members are therefore entitled to damages available under BIPA, including liquidated damages of $1,000 for each and every negligent violation, or

alternatively, $5,000 for each and every intentional or reckless violation, or actual damages, whichever is greater, injunctive relief, and further damages and relief as set forth in the PRAYER FOR RELIEF below. 740 ILCS 14/20(1)-(4).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes, pray for judgment against CenterEdge, SZFG, and Innovative Heights, as follows:

A. Certifying the CenterEdge Class, SZFG Class, and Innovative Heights Class, as requested herein;

B. Entering an order appointing Law Office of Richard S. Cornfeld, LLC and Goldenberg Heller & Antognoli, P.C. as lead counsel for the Classes;

C. Awarding statutory damages of $5,000 for each and every violation if the Court finds that CenterEdge's and/or SZFG's and/or Innovative Heights' violations were intentional or reckless, or, alternatively, statutory damages of $1,000 for each and every negligent violation of BIPA by each Defendant;

D. Awarding actual damages to Plaintiff and the members of the Classes if greater than liquidated damages, as provided for under BIPA;

E. Awarding injunctive or other equitable relief as required to protect the interests of Plaintiff and Members of the Classes, including, but not limited to, an order requiring each Defendant to permanently delete biometric data that was possessed, collected, captured, purchased, received through trade, or otherwise obtained in violation of BIPA;

F. Awarding pre-judgment and post-judgment interest;

G. Awarding reasonable attorneys' fees and costs herein; and

H. Awarding such other and further relief as the court deems fit and proper.

Dated: September 1, 2022

Respectfully submitted,

GOLDENBERG HELLER & ANTOGNOLI, P.C.

By: */s/ Kevin P. Green*
Kevin P. Green, #6299905
Thomas C. Horscroft, #06327049
2227 South State Route 157
Edwardsville, ILL 62025
Telephone: (618) 656-5150
kevin@ghalaw.com
thorscroft@ghalaw.com

Richard S. Cornfeld, #0519391
Daniel S. Levy, #6315524
LAW OFFICE OF RICHARD S. CORNFELD, LLC
1010 Market Street, Suite 1645
St. Louis, MO 63101
P. 314-241-5799
F. 314-241-5788
rcornfeld@cornfeldlegal.com
dlevy@cornfeldlegal.com

Attorneys for Plaintiff

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on August 19, 2022, a redacted version of this Third Amended Complaint was electronically with the Clerk of Court and served upon all counsel of record via the Court's electronic notification system. The undersigned further certifies that on August 19, 2022, a non-redacted version of this Third Amended Complaint was served upon all counsel of record via electronic mail. The undersigned further certifies that on September 1, 2022, pursuant to the Court's Order dated September 1, 2022 (Doc. 150), this non-redacted version of the Third Amended Complaint was filed electronically with the Clerk of Court and served upon all counsel of record via the Court's electronic notification system.

/s/ Kevin P. Green