☐ YES ☑ NO

EXHIBITS

CASE NO. 2021 CH 3460

DATE: 7/15/2021

CASE TYPE: Class Action

PAGE COUNT: 22

CASE NOTE

_____

_____

_____

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

EBONY JONES and MARLA WALKER, *individually and on behalf of all others similarly situated*,

Plaintiffs,

v.

LEMONADE INC.,

Defendant.

Case No. 2021CH03460

CLASS ACTION COMPLAINT

Plaintiffs Ebony Jones and Marla Walker, individually and on behalf of all other persons similarly situated (collectively, "Plaintiffs"), by and through their undersigned attorneys, as and for their Class Action Complaint asserting violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. ("BIPA") against Lemonade Inc. ("Lemonade" or "Defendant"), allege on personal knowledge, due investigation of their counsel and, where indicated, on information and belief as follows:

NATURE OF THE ACTION

1. Every individual has unique biometric identifiers by which he or she can be identified. One such biometric identifier is a person's facial geometry.

2. The collection, storage, use and dissemination of such sensitive information is highly controversial.

3. The State of Illinois has been at the forefront of protecting its residents from the surreptitious collection, storage, use, sale, and dissemination of their immutable biometric information.

4. Passed in 2008, the BIPA confers on *all* Illinois residents, among other things, a right to know of the risks and dangers presented by the collection, storage and use of their immutable biometric identifiers[1] and biometric information[2] (referred to collectively at times as "biometrics"), as well as a right to have their biometrics stored using a reasonable standard of care and in a manner that is as protective (if not more so) than the manner in which entities store other confidential information.

5. As the Illinois General Assembly found: "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."

6. Particularly pertinent in this case, businesses worldwide continue to develop ever more advanced facial recognition technology in order to, among other things, gain competitive advantages in the marketplace. This race for data imperils the privacy of individuals everywhere.

7. Public policy in Illinois provides that, given the risks of such unwanted data collection and disclosure, citizens need the power to make decisions about the fate of their unique biometric identifiers and information. And, in order for such power not to be illusory, Illinois residents need to be informed by companies that seek to collect and use their biometric information.

[1] A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA and "face geometry," among others.

[2] "Biometric information" is any information captured, converted, stored or shared based on a person's biometric identifier used to identify an individual.

8. Plaintiffs bring this privacy class action lawsuit against Lemonade, a digital, artificial-intelligence driven insurance company that boasts about its ability to extract thousands of bits of data from videos it requires its customers to upload in order to process their insurance claims.

9. As set forth herein, Lemonade collected Plaintiffs' and the Class Members' biometric identifiers and biometric information, including their facial geometry via videos it required its customers to upload via its mobile application (the "App").

10. Despite the fact that BIPA has been the law of the State of Illinois since 2008, and the fact that Lemonade professes to be extremely protective of its customers' personal information, it never adequately informed Plaintiffs or the Class of its biometrics collection practices, never obtained the requisite written consent from Plaintiffs or the Class to collect, store, use and disseminate their biometric information, including facial geometry, and never made public any data retention or destruction policies to Plaintiffs or the Class.

11. Plaintiffs therefore bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Lemonade in collecting, storing, and using their and other similarly situated individuals' biometrics without obtaining prior, informed written consent or providing the requisite data retention and destruction policies, in direct violation of BIPA.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this lawsuit as the Illinois Constitution gives trial courts subject matter jurisdiction over all justiciable matters.

13. This Court may assert personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States

because Defendant Lemonade—a publicly-traded company incorporated in Delaware with its principal place of business in New York—does business in the State of Illinois.

14. Moreover, the exercise of personal jurisdiction over Lemonade is appropriate because it collected, stored, and used biometric information and identifiers from Illinois residents who used the Lemonade App and thereby exposed residents of Illinois to ongoing privacy risks.

15. Furthermore, many of the images Lemonade used for its unlawful collection, storage and use of biometric identifiers and information were created in Illinois, uploaded from Illinois and/or managed via Illinois residents' user accounts, computers, and mobile devices. Because of the scope and magnitude of its conduct, Lemonade knew that its collection, storage, use, disclosure and dissemination of impacted individuals' biometric identifiers and information would injure Illinois residents and citizens.

16. Lemonade knew or had reason to know that collecting, storing, using, disclosing and disseminating Illinois citizens' and residents' biometric identifiers and information without providing the requisite notice or obtaining the requisite written releases would deprive Illinois citizens and residents of their statutorily-protected privacy rights, neutralize Illinois citizens' and residents' ability to control access to their biometric identifiers and information via the devices they managed from Illinois and expose Illinois' residents to potential surveillance and other privacy harms as they went about their lives within the State.

17. Venue is proper in this County pursuant to 735 ILCS 5/2-102(a) because Defendant conducts usual and customary business in Cook County, and many of the acts complained about herein occurred in Cook County.

PARTIES

18. Plaintiff Ebony Jones is, and has been at all relevant times, a resident of Elgin, Illinois, and a citizen of the State of Illinois.

19. Plaintiff Marla Walker is, and has been at all relevant times, a resident of Skokie, Illinois, and a citizen of the State of Illinois.

20. Defendant Lemonade Inc. is a fully licensed and regulated insurance company which underwrites, prices, and sells various insurance policies. Lemonade is incorporated in the State of Delaware and has its principal place of business in New York, New York. Lemonade is a public company traded under the ticker symbol LMND.

FACTUAL BACKGROUND

I. Illinois' Biometric Information Privacy Act.

21. Recognizing the need to protect its citizens from the risks of unauthorized access to, collection, use and disclosure of their immutable biometric information, Illinois enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*, in 2008, to regulate companies that collect and store biometric information, such as facial geometry. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276.

22. In promulgating BIPA, the Illinois Legislature found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information" because "[b]iometrics[] are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *See* 740 ILCS 14/15(c).

23. The BIPA attempts to address these issues by requiring that entities like Defendant may not, *inter alia*, obtain and/or possess an individual's biometrics unless it informs that person

in writing that biometric identifiers or information will be collected or stored. *See* 740 ILCS 14/15(b).

24. The BIPA further requires that entities collecting biometrics must inform those persons in writing of the specific purpose and length of term for which such biometric identifiers or biometric information are being collected, stored, and used. *See id.*

25. Moreover, entities collecting biometrics must publish publicly available written retention schedules and guidelines for permanently destroying biometrics collected. *See* 740 ILCS 14/15(a).

26. Further, the entity must store, transmit and protect an individual's biometric identifiers and biometric information using the same standard of care in the industry and in a manner at least as protective as the means used to protect other confidential and sensitive information. *See* 740 ILCS 14/15(c).

27. Finally, such entity is expressly prohibited from selling, leasing, trading or otherwise profiting from an individual's biometrics. *See* 740 ILCS 15/15(c).

28. In direct violation of each of the foregoing provisions of §§15(a) and 15(b) of BIPA, Lemonade collected, stored, and used—without first providing notice, obtaining informed written consent or publishing data retention policies—the biometrics and associated personally identifying information of thousands of Illinois residents who were forced to use Lemonade's App to upload videos in order to have their insurance claims processed.

II. Lemonade Collects, Stores and Uses Illinois' Residents' Protected Biometric Information and Identifiers.

29. Defendant Lemonade is a fast-growing, publicly traded insurance company that prides itself on its pioneering use of artificial intelligence ("AI") and other technologies to intake

and to process insurance claims.[3]

30. Based in and originally launched in New York, Lemonade uses an AI-powered app that offers homeowners, renters, pet and life insurance policies.

31. Lemonade began writing policies in the State of Illinois in or about April of 2017.

32. By the end of 2020, Lemonade had in excess of 1,000,000 customers in the United States, and its Chief Operating Officer boasted:

> With every new customer, our system grows smarter, our underwriting process gets better, and our prices become more accurate and fair. **At Lemonade, one million customers translates into billions of data points, which feed our AI at an ever growing speed. Quantity generates quality.**[4]

33. One of the ways that Lemonade is able to collect so much of its customers' biometric and other information is by using its APP to collect and to maintain vast troves of customer information, including biometric information.

34. Lemonade is unique in the insurance industry in that its customers (its policy holders) are required, in connection with their claims submission, to upload a video message describing what happened and the facts upon which their claim is based.[5]

35. Notably, the video is not essential or even necessary to the claim submission, which is completed via a "chat-bot" in the App. Rather, Lemonade requires its customers to provide a video of themselves through the App in order to acquire thousands and thousands of "bits" of data so that Lemonade can then decide whether to honor a given claim and how to price its insurance

---

[3] *See* https://www.vox.com/recode/22455140/lemonade-insurance-ai-twitter (last visited July 15, 2021).

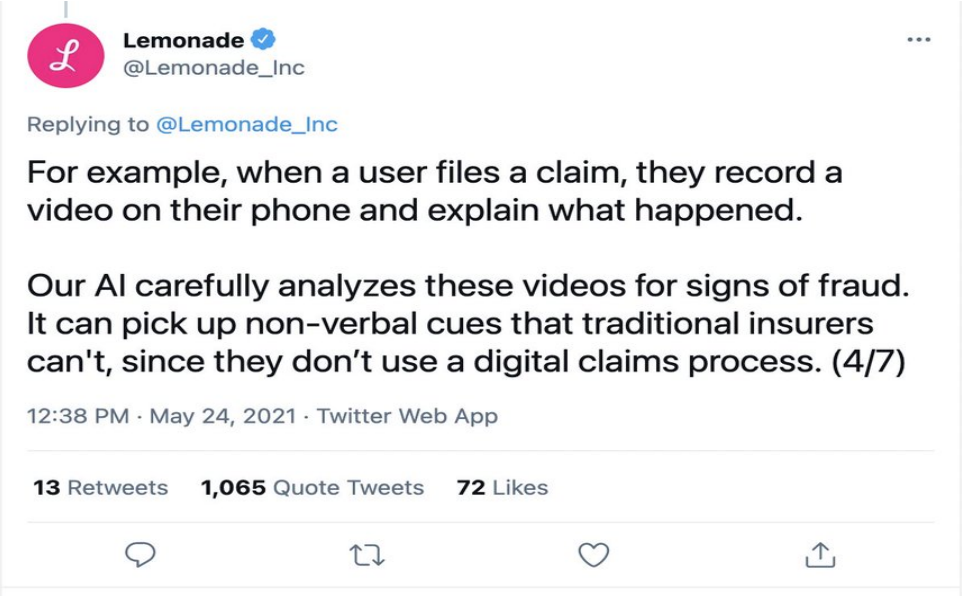
[4] *See* https://finance.yahoo.com/news/lemonade-ends-2020-over-one-134600018.html (last visited July 15, 2021) (emphasis added).

[5] *See* https://frankonfraud.com/fraud-trends/lemonade-under-fire-for-using-ai-to-stop-insurance-fraud/#:~:text=Lemonade%2C%20(not%20the%20drink),claims%20if%20they%20suspect%20fraud (last visited July 15, 2021).

products.

36. Lest there be any doubt about its intentions, Lemonade itself made them quite clear when it issued a series of tweets containing a proud declaration that its AI analyzes videos of customers when determining if their claims are fraudulent.[6]

37. Lemonade announced that its customer service chatbots collect as many as 1,600 data points from a single video of a customer answering questions regarding their claim:



38. Lemonade's twitter thread "implied that [it] was able to detect whether a person was lying in their video and could thus decline insurance claims if its AI believed a person was lying."[7]

39. Lemonade has boasted that it collects "100X more data than traditional insurance carriers."[8]

40. Later that week, Lemonade clarified its controversial tweet, explaining that "[t]he

[6] https://www.vox.com/recode/22455140/lemonade-insurance-ai-twitter (last visited July 15, 2021).

[7] https://frankonfraud.com/fraud-trends/lemonade-under-fire-for-using-ai-to-stop-insurance-fraud/.

[8] https://www.vox.com/recode/22455140/lemonade-insurance-ai-twitter.

term, non-verbal cues was a bad choice of words to describe **the facial recognition technology we're using** to flag claims submitted by the same person under different identities. These flagged claims then get reviewed by our human investigators."[9]

41. Thus, Lemonade confirmed that it uses *facial recognition technology to collect reams of data, including biometric data like face geometry, from its customers, including those in the State of Illinois.*

42. In a post authored by its Chief Executive Officer and shared on its blog, Lemonade stated:

> It's different for companies built on a digital substrate. Lemonade's chatbots do away with forms altogether, making the process fast and fun, but the data implications are still more profound:
>
> *Lemonade collects about 100x more data-points per customer.*
>
> That's the power of an entirely digital experience.[10]

43. Indeed, as a recent article detailing Lemonade's questionable uses of AI makes explains, "[t]he in-depth collection of video data and analyzing it against AI tools **make it clear that Lemonade must be storing at least some biometric data** in order to train models to detect patterns of fraud."[11]

44. Or, put another way, Lemonade is an insurance company that claims it is replacing human brokers and actuaries with bots and AI in order to streamline the insurance claim process. In the process, however, Lemonade collects tremendous amounts of data, including biometric

---

[9] https://www.lemonade.com/blog/lemonades-claim-automation/ (last visited July 15, 2021) (emphasis added).

[10] https://www.lemonade.com/blog/precision-underwriting/ (last visited July 15, 2021) (emphasis in original).

[11] https://frankonfraud.com/fraud-trends/lemonade-under-fire-for-using-ai-to-stop-insurance-fraud/.

information, about its customers without telling them in direct violation of BIPA.[12]

45. For instance, an article published in *Forbes* detailed a situation where Lemonade used facial recognition technology to compare various claims submitted by customers in order to root out fraud:

> In the summer of 2017, a Los Angeles man in his mid-20s put on a necklace, blond wig and makeup and made a cellphone video describing how his camera and other electronics had been stolen. He submitted the video to his renters insurance provider, Lemonade, which paid the $677 claim in two days. Three months later, dressed in jeans and a T-shirt and using a different name, email address and phone number, the same man submitted a video claim for a stolen $5,000 camera. But this time, the algorithms that are a crucial part of Lemonade's highly automated systems flagged the claim as suspicious. Last year, the persistent fraudster, this time wearing a pink dress, tried again, only to be foiled once more by Lemonade's computers.[13]

46. Lemonade used its AI, including facial recognition technology, to determine that the claimants in the above scenario were the same person by collecting, storing, and using the immutable biometric information and identifiers of its customers.[14]

47. In its S-1 form filed with the U.S. Securities and Exchange Commission prior to the company going public—and in forms since—Lemonade states that its proprietary AI algorithms are at the core of its business and that it could not function without them, but admits that they could also lead to profit loss should regulators ever crack down:

> ***Our proprietary artificial intelligence algorithms may not operate properly or as we expect them to***, which could cause us to write policies we should not write, price those policies inappropriately or

[12] https://www.vox.com/recode/22455140/lemonade-insurance-ai-twitter

[13] https://www.forbes.com/sites/jeffkauflin/2019/05/02/lemonade-fintech-insurance-unicorn/?sh=23c5a7ee6cde (last visited July 15, 2021).

[14] https://frankonfraud.com/fraud-trends/lemonade-under-fire-for-using-ai-to-stop-insurance-fraud/ (stating that "[t]he in-depth collection of video data and analyzing it against AI tools make it clear that Lemonade must be storing at least some biometric data in order to train models to detect patterns of fraud").

> overpay claims that are made by our customers, the company wrote in the filing. Moreover, our proprietary artificial intelligence algorithms may lead to unintentional bias and discrimination.[15]

48. In short, Lemonade did not disclose to its customers the extent to which it was collecting and using their sensitive biometric (and other information). Indeed, the "instant, seamless, and delightful" insurance experience that Lemonade aggressively markets was built by the collection of its customers' own data, including their biometric information, which those customers never realized they were providing.

49. As noted in a recent article entitled *A disturbing, viral Twitter thread reveals how AI-powered insurance can go wrong*, *Lemonade tweeted about what it means to be an AI-first insurance company. It left a sour taste in many customers' mouths*:

> It's rare for a company to be so blatant about how that data can be used in its own best interests and at the customer's expense. But rest assured that Lemonade is not the only company doing it.[16]

50. According to the analytics site, Crunchbase, there were 47,345 downloads of the App in the last thirty days (as of July 13, 2021), representing a nearly 5% increase from the prior thirty-day period.[17]

III. Lemonade's Conduct Violates the BIPA.

51. As detailed above, Lemonade designed and implemented an AI tool in the App that automatically performs facial scans, collecting the facial geometry of customers who use the App.

52. In collecting, using, storing and otherwise obtaining the biometric identifiers and information of Plaintiffs and the Class Members and, upon information and belief, subsequently

---

[15] https://www.vice.com/en/article/z3x47y/an-insurance-startup-bragged-it-uses-ai-to-detect-fraud-it-didnt-go-well (emphasis added).

[16] https://www.vox.com/recode/22455140/lemonade-insurance-ai-twitter.

[17] https://www.crunchbase.com/organization/lemonade/technology (last visited July 13, 2021).

disclosing, re-disclosing and otherwise disseminating those biometric identifiers and information to other related corporate entities—all without providing the requisite notice, obtaining the requisite written releases or satisfying any of the other provisions that would excuse it from BIPA's mandates—Lemonade violated BIPA.

53. In further violation of BIPA, Lemonade failed to use a reasonable standard of care to protect Plaintiffs' and Class Members' biometric identifiers and information from disclosure.

54. In further violation of BIPA, as a private entity in possession of Plaintiffs' and Class Members' biometric identifiers and information, Lemonade failed to adopt or make available to the public a retention schedule or guidelines for permanently destroying such biometric identifiers and information once the initial purpose for collecting them had or has been satisfied.

55. Lemonade's violations of BIPA were intentional and reckless or, in the alternative, negligent.

IV. Experience of Representative Plaintiff Ebony Jones.

56. Plaintiff Jones, an Illinois resident, has been a Lemonade customer since at least 2020.

57. In connection with submitting an insurance claim following a weather incident which caused damage to her home, Plaintiff Jones, as required by Defendant, accessed and used Lemonade's App.

58. Plaintiff Jones answered numerous questions posed to her by a Lemonade "chat-bot." Lemonade had all the requisite information it needed to process Plaintiff Jones' claim, as well as her contact information in order to follow-up with her if it required additional information.

59. Nonetheless, Lemonade required Plaintiff Jones to upload a "short video describing the incident."

60. Plaintiff Jones uploaded a video of herself describing the incident on July 10, 2020.

61. Plaintiff Jones did not know that Lemonade would collect, obtain, store and/or use her biometric identifiers or biometric information.

62. Plaintiff Jones did not give informed written consent to Lemonade to collect, obtain, store and/or use her biometric identifiers or biometric information, nor was Plaintiff Jones presented with or made aware of any publicly available retention schedule regarding her biometric identifiers or biometric information.

63. Likewise, Lemonade never provided Plaintiff Jones with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of her unique biometric identifiers and/or biometric information.

64. By collecting, obtaining, storing, and using Plaintiff Jones's unique biometric identifiers and/or biometric information without her consent, written or otherwise, Lemonade invaded Plaintiff Jones's statutorily protected right to privacy in her biometrics.

65. In direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, Lemonade never informed Illinois residents who had their biometrics collected of the specific purpose and length of time for which their biometric identifiers or information would be collected, stored, and used, nor did Defendant obtain a written release from these individuals.

66. In direct violation of § 15(a) of BIPA, Lemonade did not have written, publicly available policies identifying their retention schedules or guidelines for permanently destroying any of these biometric identifiers and/or biometric information.

V. Experience of Representative Plaintiff Marla Walker.

67. Plaintiff Walker, an Illinois resident, has been a Lemonade customer since at least 2018.

68. In connection with submitting an insurance claim in or around September 2018, Plaintiff Walker, as required, accessed, and used Lemonade's App.

69. In so doing, Plaintiff Walker answered numerous questions posed to her by a Lemonade "chat-bot." Lemonade had all the requisite information it needed to process Plaintiff Walker's claim, as well as her contact information in order to follow up with her if it required additional information.

70. Nonetheless, Lemonade required Plaintiff Walker to upload a "short video describing the incident."

71. Plaintiff Walker uploaded a video of herself describing the incident on or about September 15, 2018.

72. Plaintiff Walker did not know that Lemonade would collect, obtain, store and/or use her biometric identifiers or biometric information.

73. Plaintiff Walker did not give informed written consent to Lemonade to collect, obtain, store and/or use her biometric identifiers or biometric information, nor was Plaintiff Walker presented with or made aware of any publicly available retention schedule regarding her biometric identifies or biometric information.

74. Likewise, Lemonade never provided Plaintiff Walker with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage or use of her unique biometric identifiers and/or biometric information.

75. By collecting, obtaining, storing, and using Plaintiff Walker's unique biometric identifiers and/or biometric information without her consent, written or otherwise, Lemonade invaded Plaintiff Walker's statutorily protected right to privacy in her biometrics.

76. In direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, Lemonade never informed

Illinois residents who had their biometrics collected of the specific purpose and length of time for which their biometric identifiers or information would be collected, stored and used, nor did it obtain a written release from these individuals.

77. In direct violation of § 15(a) of BIPA, Lemonade did not have written, publicly available policies identifying their retention schedules or guidelines for permanently destroying any of these biometric identifiers and/or biometric information.

CLASS ALLEGATIONS

78. **Class Definition:** Plaintiffs bring this action pursuant to 735 ILCS 5/2-801 on behalf of a class of similarly situated individuals, defined as follows:

> All individuals whose biometric identifiers or biometric information were collected, captured, stored, used, transmitted, received or otherwise obtained and/or disseminated by Lemonade within the State of Illinois within the applicable limitations period (the "Class").

79. Excluded from the Class are (i) any members of the judiciary assigned to preside over this Matter, as well as their immediate family members, (ii) any officer or director of Defendant and any immediate family members of such officer or director; (iii) any entity in which Defendant have a controlling interest and (iv) any employees and agents of Defendant.

80. **Numerosity:** Pursuant to 735 ILCS 5/2-801(1), the number of persons within the Class is substantial, believed to amount to thousands of persons. It is, therefore, impractical to join each Member of the Class as a named Plaintiff. Further, the size and relatively modest value of the claims of the individual Members of the Class render joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, membership in the Class is readily ascertainable and identifiable from Lemonade's records.

81. **Commonality and Predominance:** Pursuant to 735 ILCS 5/2-801(2), there are

well-defined common questions of fact and law that exist as to all Members of the Class and that predominate over any questions affecting only individual Members of the Class. These common legal and factual questions, which do not vary from Class Member to Class Member, and which may be determined without reference to the individual circumstances of any Class Member, include, but are not limited to, the following:

(a) whether Defendant collected or otherwise obtained Plaintiffs' and the Class Members' biometric identifiers and/or biometric information;

(b) whether Defendant properly informed Plaintiffs and the Class Members that they collected, used, and stored their biometric identifiers and/or biometric information;

(c) whether Defendant obtained a written release (as defined in 740 ILCS 1410) to collect, use and store Plaintiffs' and the Class Members' biometric identifiers and/or biometric information;

(d) 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 3 years of their last interaction, whichever occurs first;

(e) whether Defendant used Plaintiffs' and the Class Members' biometric identifiers and/or biometric information to identify them;

(f) whether Defendant destroyed Plaintiffs' and the Class Members' biometric identifiers and/or biometric information once that information was no longer needed for the purpose for which it was originally collected and

(g) whether Defendant's violations of BIPA were committed intentionally, recklessly or negligently.

82. **Adequate Representation:** Pursuant to 735 ILCS 5/2-801(3), Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in

complex consumer class action litigation. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiffs are able to fairly and adequately represent and protect the interests of the Class. Neither Plaintiffs nor their counsel have any interest adverse to, or in conflict with, the interests of the absent Members of the Class. Plaintiffs have raised viable statutory claims, or the type reasonably expected to be raised by Members of the Class, and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Class, additional claims as may be appropriate and/or to amend the Class definition.

83. **Superiority:** Pursuant to 735 ILCS 5/2-801(4), a class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class Members is impracticable. Even if every Member of the Classes could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent ,or contradictory judgments and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each Member of the Class. Plaintiffs anticipate no difficulty in the management of this action as a class action.

84. In short, maintenance of this case as a class action is essential to compliance with BIPA.

COUNT I – FOR DAMAGES AGAINST DEFENDANT
VIOLATION OF 740 ILCS 14/15(a) – FAILURE TO INSTITUTE, MAINTAIN AND ADHERE TO PUBLICLY AVAILABLE RETENTION SCHEDULE

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

86. BIPA mandates that entities in possession of biometric data establish and maintain a satisfactory biometric data retention—and, importantly, deletion—policy.

87. Specifically, those entities 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 entity'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).

88. Defendant did not comply with these BIPA mandates.

89. Defendant Lemonade is a company registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See id*.

90. Plaintiffs are individuals who had their "biometric identifiers" captured and/or collected by Defendant, as explained in detail herein. *See id*.

91. Plaintiffs' and the Class Members' biometric identifiers were used to identify them and therefore constitute "biometric information" as defined by BIPA. *See id.*

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

93. Defendant lacked retention schedules and guidelines for permanently destroying Plaintiffs' and the Class Members' biometric data. As such, the only reasonable conclusion is that Defendant has not, and will not, destroy Plaintiffs' and the Class Members' biometric data when the initial purpose for collecting or obtaining such data has been satisfied.

94. On behalf of themselves and the Class, Plaintiffs seek: (i) declaratory relief; (ii) 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, capture, storage and use of biometric identifiers and biometric information as described herein; (iii) 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 (iv) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT II – FOR DAMAGES AGAINST DEFENDANT
VIOLATION OF 740 ILCS 14/15(b) – FAILURE TO OBTAIN INFORMED WRITTEN CONSENT AND RELEASE BEFORE OBTAINING BIOMETRIC IDENTIFIERS OR INFORMATION

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

96. BIPA requires entities to obtain informed written consent from Illinois residents before acquiring their biometric data.

97. 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: (i) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (ii) 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** (iii) receives a written release executed by the subject of the biometric identifier or biometric information . . . " 740 ILCS 14/15(b) (emphasis added).

98. Defendant did not comply with these BIPA mandates.

99. Defendant Lemonade, Inc. is a company registered to do business in Illinois and

thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

100. Plaintiffs and the Class Members are individuals who have had their "biometric identifiers" collected and/or captured by Defendant, as explained herein. *See id*.

101. Plaintiffs' and the Class Members' biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See id.*

102. Defendant systematically and automatically collected, captured, used, and stored 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).

103. Defendant never informed Plaintiffs, and never informed any Member of the Class in writing that their biometric identifiers and/or biometric information were being collected, captured, stored, and/or used, nor did Defendant inform Plaintiffs and the Class in writing of the specific purpose(s) and length of term for which their biometric identifiers and/or biometric information were being collected, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

104. By collecting, capturing, storing, and/or using Plaintiffs' and the Class Members' biometric identifiers and biometric information as described herein, Defendant violated Plaintiffs' and the Class Members' 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 themselves and the Class, Plaintiffs seek: (i) declaratory relief; (ii) 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, capture, storage, use and dissemination of biometric identifiers and biometric information as described herein; (iii) 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 (iv) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Ebony Jones and Marla Walker, on behalf of themselves and the proposed Class, 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 as representatives of the Class and appointing their counsel as Class Counsel;

B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq*.;

C. Awarding statutory damages of $5,000.00 for each and every intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, alternatively, statutory damages of $1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if the Court finds that Defendant's violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an Order requiring Defendant to collect, store and use biometric identifiers and/or biometric information in compliance with BIPA;

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

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

G. Awarding all such other and further relief as equity and justice may require.

Dated: July 15, 2021

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Phone: (202) 429-2290
Fax: (202) 429-2294
gklinger@masonllp.com

Gary E. Mason*
David K. Lietz*
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Phone: (202) 429-2290
Fax: (202) 429-2294
gmason@masonllp.com
dlietz@masonllp.com

Attorneys for Plaintiffs & the Proposed Class

**Pro Hac Vice* forthcoming

ClassAction.org