IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

DAVID KARLING, *individually and on behalf all others similarly situated,*	)	
	)	Case No. 1:22-cv-00295
Plaintiff,	)	Hon. Georgia N. Alexakis
v.	)	
SAMSARA INC., *a Delaware Corporation,*	)	
Defendant.	)	

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiff David Karling ("Plaintiff"), individually and on behalf of all other persons similarly situated, by and through his attorneys, brings this Second Amended Class Action Complaint for violations of the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq*., against Defendant Samsara Inc. ("Samsara") and alleges on personal knowledge, due investigation of his counsel, and, where indicated, on information and belief as follows:

NATURE OF THE ACTION

1. Samsara is a technology company that licenses facial recognition software to commercial fleets and industrial operations to monitor and identify their drivers. Samsara operates that technology through an inward-facing dashboard camera, and Plaintiff alleges that a central feature of this camera, called Camera ID, violates BIPA.

2. Camera ID uses the inward-facing camera to identify who is driving a vehicle. To do so, according to Samsara's website, it "rel[ies] on facial recognition information derived from

images of drivers."[1]

3. After obtaining images of a driver's face through its Camera ID feature, Samsara sends an image of the driver's face to its agent, Amazon Web Services ("AWS"), to scan the driver's face against a database of faces belonging to that driver and their colleagues to determine who is driving.

4. To perform this facial recognition process, [redacted]

5. [redacted]

6. Plaintiff and similarly situated Class Members did not consent to this collection of their biometric information[2] and biometric identifiers[3] (collectively, "biometrics") in violation of BIPA.

[1] Special Feature, https://www.samsara.com/support/privacy/special-features (last visited October 12, 2023).

[2] "Biometric information" is "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.

[3] "Biometric identifier" means "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

7. Samsara's actions violate four separate provisions of BIPA:

a. Samsara's written policy on retention schedules and guidelines for permanently destroying the biometrics it collects violates BIPA because it fails to inform the public about its actual retention schedule and guidelines for permanently destroying biometric information. *See* 740 ILCS 14/15(a).[4] Further, [redacted]. *Id.*

b. Samsara, on its own and with its agent, AWS, collects drivers' biometric information in violation of 740 ILCS 14/15(b). Further, Samsara has not obtained written consent from a single driver, including Plaintiff. Samsara's position that its customers can obtain blanket consent for themselves and Samsara fails both legally and factually. Legally, BIPA requires Samsara itself to obtain its own consent. Factually, discovery to date reveals that [redacted].[5]

c. Samsara, on its own and through agent AWS, violates 740 ILCS 14/15(c) because when it licenses the use of its inward-facing cameras to its customers—for example, transportation companies like Plaintiff's employer—it profits from being able to track Plaintiff's and similarly situated individuals' biometrics. Biometrics are a necessary element of Samsara's

[4] [redacted] Samsara_00020. The Court previously considered this policy in its July 2022 motion to dismiss order and held that "the website says nothing about destruction guidelines." Dkt. 25, at 10-11.

[5] Samsara_001186.

business model, and by marketing its cameras and services, Samsara is commercially disseminating the biometrics. *See* 740 ILCS 14/15(c).

d. Finally, Samsara, on its own and through AWS, violates Plaintiff's and other similarly situated individuals' rights when it discloses, rediscloses, or otherwise disseminates drivers' biometric identifiers or biometric information to drivers' employers without drivers' informed consent. *See* 740 ILCS 14/15(d).

PARTIES

8. Plaintiff David Karling is, and has been at all relevant times, a resident and citizen of Illinois.

9. Defendant Samsara Inc. is a corporation organized and existing under the laws of the State of Delaware and is headquartered in the State of California.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d) and the Class Action Fairness Act because the amount in controversy exceeds $5,000,000, and Samsara is a citizen of California and is therefore diverse from at least one Plaintiff.

11. This Court has personal jurisdiction over Samsara because Samsara is authorized to do business in this District, conducts substantial business in this District, and the actions giving rise to the complaint took place in this District. For instance, Samsara knowingly distributed its cameras to businesses operating in Illinois and its cameras inform Samsara of where drivers are located when the camera is capturing their information, including when drivers are located in Illinois.[6] Samsara also profits from biometrics collected from individuals physically present in Illinois.

[6] Samsara_0004. Samsara previously did not contest personal jurisdiction in moving to dismiss Plaintiff Karling's lawsuit in 2022. Dkt. 15.

12. Each of these facts independently is, and all of these facts together are, sufficient to render the exercise of jurisdiction by this Court over Samsara permissible under traditional notions of fair play and substantial justice.

FACTUAL BACKGROUND

I. The Illinois Biometric Information Privacy Act.

13. In 2008, Illinois enacted BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276.

14. The Illinois Legislature codified within BIPA that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "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." *Id.*

15. To protect the public from these risks and serve the "public welfare, security, and safety," 740 ILCS 14/5(g), the Illinois Legislature enacted BIPA.

16. BIPA protects biometric identifiers, which include retina and iris scans, voiceprints, fingerprints, scans of hand geometry, and—most importantly here—scans of face geometry (also called "face vectors"). *See* 740 ILCS 14/10. It also protects biometric information, which is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *See id*.

17. BIPA makes it unlawful for a company to, *inter alia*, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers and/or biometric information, unless it first:

> (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

740 ILCS 14/15 (b).

18. Section 15(a) of BIPA also provides:

> A 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). It also requires that "a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines." *Id.*

19. Section 15(c) of BIPA prohibits a private entity from "sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

20. Further, to disclose, redisclose, or otherwise disseminate biometric identifiers or biometric information, the entity must obtain the subject of the biometric identifier or biometric information's consent. *See* 740 ILCS 14/15(d)(1).

21. Altogether, BIPA protects individuals' biometric identifiers and biometric information by requiring private entities to follow certain prerequisites before they collect, send, transmit, or disclose the information.

II. Samsara's Inward-Facing Cameras.

22. Samsara is a publicly owned technology company founded in 2015.[7]

23. In late 2021, Samsara was listed on the New York Stock Exchange, where its stock currently trades, as of October 2023, it had a market capitalization of roughly $13 billion.[8]

24. Samsara claims that it works with 20,000 different businesses, its cameras have processed 38 billion minutes of video footage, and it collects 2 trillion data points yearly.[9] In Illinois, Samsara represented that "approximately 49,000 drivers employed by Samsara's customers…currently have Camera ID enabled and began a trip in the state of Illinois."[10]

25. Relevant here, Samsara licenses a "Dual-Facing AI Dash Cam" ("Dash Cam") to commercial freight companies. The Dash Cam combines footage of drivers' faces and "advanced machine learning" to identify drivers, monitor their faces for signs of drowsiness or distracted driving, and associate "safety events" with individual drivers.[11]

26. Samsara's corporate representative and Vice President of Product Management - Safety estimated that [redacted].[12]

---

[7] https://www.samsara.com/company/about (last visited Oct. 12, 2023).

[8] https://finance.yahoo.com/quote/IOT/ (last visited Oct. 12, 2023).

[9] https://www.samsara.com/blog/samsara-engineering-culture (last visited Oct. 14, 2023); https://www.samsara.com/pages/thesamsaraadvantage/ (last visited Oct. 14, 2023).

[10] Samsara's Amended Responses to Plaintiff's Amended First Set of Interrogatories, Apr. 7, 2023, ROG 14.

[11] Samsara_00001, Automatic Driver Detection (Camera ID); Samsara_00023, AI Event Detection.

[12] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 105:3-10; 109:1-5.

27. [redacted].[13]

28. [redacted].[14]

29. As part of its package to trucking companies like Plaintiff's employer, Samsara hosts, maintains, and provides access to its cloud-based software, the "Samsara Cloud Dashboard."[15]

30. Through the Dashboard, [redacted].[16]

31. Samsara's cloud storage is hosted through AWS as well, using its Amazon S3 product.[17] Upon information and belief, all driver biometric data collected by Samsara is stored via Amazon S3.

32. Samsara also uses AWS's CloudFront, "a content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally."[18] Upon

[13] *Id.* at 33:5-8.

[14] Samsara's Supplemental Responses to Plaintiff's Third Set of Interrogatories, Sept. 28, 2023, ROG 1.

[15] Access the Samsara Dashboard, https://kb.samsara.com/hc/en-us/articles/4410663027981-Access-the-Samsara-Dashboard (last visited Oct. 14, 2023).

[16] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 117:8-12; Samsara_007218.

[17] Samsara, Security, https://www.samsara.com/legal/security/ (last visited Oct. 16, 2023).

[18] AWS Whitepapers, Introduction, https://docs.aws.amazon.com/whitepapers/latest/secure-content-delivery-amazon-cloudfront/introduction.html (last visited Oct. 16, 2023).

information and belief, Samsara uses CloudFront to deliver biometric data uploaded to the AWS cloud back to its customers upon request through the Samsara Cloud Dashboard.

33. Additionally, [redacted] .[19]

34. Plaintiff's and Class Members' biometrics are collected by Samsara and its agent AWS when trucking companies deploy the Camera ID feature.

III. Samsara's Camera ID feature collects biometrics.

[redacted]

35. Samsara defines its Camera ID feature as [redacted] .[20]

36. [redacted] .[21] [redacted] .[22]

B. How Camera ID Mechanically Works.

37. Mechanically, [redacted]

[19] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 95:11-96:5.
[20] Samsara_015454.
[21] Samsara_000117.
[22] *Id.*

[redacted][23]

[redacted][24]

39. [redacted][25]

40. [redacted].[26]

41. [redacted]

[23] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 115:2-116:5.

[24] In addition to capturing drivers' faces, internal documents produced by Samsara demonstrate that [redacted] Samsara_017268.

[25] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 117:13-118:12.

[26] Samsara's Supplemental Response to Plaintiff's Second Set of Interrogatories, Sept. 28, 2023, at ROG 2.

[redacted][27]

42. [redacted] "[A]fter identifying and assigning a driver 5-10 times to train the Camera ID, Samsara's Dash Cams will begin automatically recognizing and assigning their names with their faces with high accuracy." [28]

43. [redacted].[29]

44. The first step occurs [redacted].[30] At this point, [redacted][31]

45. Next, [redacted].[32]

[27] *Id.*

[28] DOT Compliance: Overview and Tips for Fleet Managers, Apr. 20, 2020, https://www.samsara.com/guides/dot-compliance/ (last visited Oct. 14, 2023).

[29] Samsara's Supplemental Response to Plaintiff's Amended First Set of Interrogatories, April 7, 2023, at ROG 3.

[30] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 125:23-126:16. [redacted]

[31] Samsara's Supplemental Response to Plaintiff's Second Set of Interrogatories, Sept. 28, 2023, at ROG 2; Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 97:3-13.

[32] Samsara's Supplemental Response to Plaintiff's Second Set of Interrogatories, Sept. 28, 2023, at ROG 2.

46. [redacted][33]

47. Specifically, [redacted][34]

48. [redacted][35]

49. [redacted][36]

50. [redacted].[37]

C. <u>The Technical Means by which Camera ID collects biometrics.</u>

51. Camera ID collects biometrics as follows: [redacted][38]

52. [redacted].

[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*

53. [redacted].[39]

54. AWS's Rekognition program relies on having a large database of driver biometric data to function accurately. AWS acknowledges that "hundreds of images may sometimes be required to train a custom model with high accuracy."[40] These driver images are provided by Samsara through driver data collected from its customers. The specific Rekognition services used by Samsara do not and cannot function without this input and direction from Samsara.

55. Rekognition's comparison is done by extracting "face vectors" of individuals, which are mathematical representations of an individual's face, including precise coordinates and measurements of facial features. These "face vectors," called "face prints," are biometrics unique to each individual driver.[41]

56. Thus, [redacted].[42]

57. In a recent lawsuit in the Western District of Washington against Amazon for violating BIPA through its Rekognition technology, an Amazon corporate representative

[39] AWS, *Overview of face detection and face comparison*, https://docs.aws.amazon.com/rekognition/latest/dg/face-feature-differences.html (last visited Oct. 16, 2023).

[40] Amazon Rekognition, FAQS, https://aws.amazon.com/rekognition/faqs/#:~:text=Although%20hundreds%20of%20images%20may,train%20again%20to%20iteratively%20improve (last visited Oct. 14, 2023).

[41] *Id.*; Build Your Own Face Recognition Service Using Amazon Rekognition, Aug. 14, 2017 https://aws.amazon.com/blogs/machine-learning/build-your-own-face-recognition-service-using-amazon-rekognition/ (last visited Oct. 14, 2023).

[42] AWS, *IndexFaces*, https://docs.aws.amazon.com/rekognition/latest/APIReference/API_IndexFaces.html (last visited Oct. 16, 2023).

testified, in his personal capacity in his Product Management role, that Rekognition works as follows: "And so how it works is, you can create a collection, you can call APIs to store face vectors, and the API you call to store a face vector is Index Faces. And then if you want to search against the faces, face vectors that have been stored, you can do a Search Faces API call or you can do a Search Users API call. And that will send back a similarity score between the face vectors in the image that you searched with, compared to face vectors that are stored in the collection."[43]

58. [redacted][44]

59. While Samsara has attempted to disclaim responsibility for scanning biometrics, [redacted][45] discovery in this case and publicly available documents evidence that Samsara [redacted][46]

[43] *See Dorian v. Amazon Web Services, Inc.*, 2:22-cv-00269-JHC (W.D. Wash.), Dkt. 110-1, July 18, 2023 Deposition of Sean Simmons – 30(b)(6), 40:5-21.

[44] Samsara's Supplemental Response to Plaintiff's Second Set of Interrogatories, Sept. 28, 2023, at ROG 2.

[45] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 124:14-21.

[46] Samsara's Supplemental Response to Plaintiff's Second Set of Interrogatories, Sept. 28, 2023, at ROG 2.

60. Specifically, [redacted][47]

61. Further, Samsara's corporate representative testified that [redacted][48] [redacted][49]

62. Additionally, Samsara's internal documents show that [redacted][50] [redacted][51] Put differently, [redacted].[52]

63. Put simply, landmark data is biometric facial data unique to individuals and this evidences that [redacted].

[47] Samsara_018330, at -331.
[48] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 203:14-22.
[49] *Id.* at 203:23-204:3.
[50] Samsara_15454.
[51] *Id.*
[52] As Samsara's corporate representative explained: [redacted] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 170:11-23.

D. Samsara's Control and Storage of the Biometrics.

64. While AWS provides the facial recognition platform, Samsara, through its in-house engineering department, controls the nuances of collecting, processing, and storing drivers' biometric information.

65. Samsara exclusively controls and directs whether a driver's photograph is scanned for biometrics, when and how those biometrics are used, and whether those biometrics are stored or deleted.

66. [redacted].[53] For instance, [redacted].[54]

67. [redacted][55]

68. [redacted]

[53] Samsara's Supplemental Response to Plaintiff's Second Set of Interrogatories, Sept. 28, 2023, at ROG 2.

[54] Samsara_008783 [redacted]

[55] Samsara's Supplemental Response to Plaintiff's Second Set of Interrogatories, Sept. 28, 2023, at ROG 2.

[redacted][56] [redacted]

[redacted].[57]

69. [redacted]

[redacted]

[redacted].[58]

70. [redacted]

[redacted] The data for Camera ID is "securely stored and protected in line with all of our other Samsara cloud data."[59] [redacted]

[redacted].[60]

IV. Samsara violates four prongs of the Illinois' Biometric Information Privacy Act.

A. Samsara failed to establish and adhere to BIPA's written destruction policy requirement.

71. BIPA requires Samsara to: "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. Absent 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." 740 ILCS 14/15(a).

[56] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 96:6-97:6.
[57] Samsara_007218.
[58] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 137:21-138:7.
[59] Samsara_00001, Automatic Driver Detection (Camera ID).
[60] Rule 30(b)(6) Deposition of Ingo Wiegand, Sept. 29, 2023, at 97:18-98:4

72. Put differently, Section 15(a) imposes two requirements on Samsara—to develop a written, publicly available public with a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information and to comply with its policy. Samsara fails on both accounts.

73. Samsara's website, in a portion titled "Special Features: About Camera ID Technology," stated until October 2023 that it "keeps facial recognition information for a customer no longer than necessary to provide its Camera ID service to that customer. To delete facial recognition information stored by Samsara, contact customer support."[61]

74. This policy fails to adhere to BIPA's requirements in three ways. First, it does not establish a retention schedule. It merely states that it "keeps facial recognition information for a customer no longer than necessary."[62] What "necessary" means in this circumstance is unknowable to the public or to individuals who have had their information collected by Samsara.

75. Second, it fails to contain "guidelines for permanent destruction" because "no longer than necessary" is again an unknowable standard that could differ between unstated customer needs.[63] There is no way for Plaintiff and Class Members to know whether the guidelines for permanent destruction have been met.

76. Third, it fails to "permanently destroy" the biometric identifiers based on the stated language. The first sentence: "Samsara keeps facial recognition information for a customer no longer than necessary to provide its Camera ID service to that customer" is inconsistent with the second sentence, "to delete facial recognition information stored by Samsara, contact

[61] Special Features, https://www.samsara.com/support/privacy/special-features (last visited Oct. 16, 2023).

[62] *Id.*

[63] *Id.*

customer support."[64] Plaintiff and Class Members cannot know whether Samsara deletes information when it is "no longer necessary" or if they must "contact customer support" to have their information deleted.[65] And neither sentence demonstrates that the destruction is *permanent*.

77. The Court previously analyzed Samsara's policy in its motion to dismiss order and held that "the website says nothing about destruction guidelines." Dkt. 25 at 11.

78. Moreover, [redacted] [66] Samsara subsequently [redacted] [67]

79. In addition to failing to meet BIPA's requirements for the terms of its destruction policy, Samsara did not adhere to BIPA's requirement that it "comply with its established retention schedule and destruction guidelines." 740 ILCS 14/15(a).

80. Specifically, [redacted].

81. [redacted]

[64] *Id.*
[65] *Id.*
[66] Samsara_000838.
[67] Samsara_019476 (emphasis added).

[redacted][68] Put differently, [redacted][69]

82. [redacted][71]

83. Samsara failed to comply with its own policy, which stated that contacting Samsara customer support would result in the deletion of a driver's data.

84. [redacted][72]

85. AWS, Samsara's agent, likewise has no publicly available data retention policy covering the biometric data of Samsara's customers.

[68] Samsara_000671.
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] Samsara_018149.

B. Samsara failed to obtain the requisite consent under BIPA to collect Plaintiff and Class Members' biometric information.

86. BIPA requires Samsara, because it is an entity that collects and captures Plaintiff's and Class Members' biometric identifiers and biometric information to first: "(1) inform[] the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) inform[] the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receive[] a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." 740 ILCS 14/15(b).

1. Samsara failed to obtain consent from drivers who had their biometrics captured through Samsara's Camera ID feature.

87. Samsara never obtained consent from Plaintiff to collect his biometric identifiers and biometric information. [redacted]"[73] Samsara nevertheless failed to obtain consent.

88. Instead, Samsara takes the position that it bears no responsibility for obtaining written consent for drivers whose employers have Camera ID enabled despite collecting Plaintiff and Class Members' biometric information and biometric identifiers.

89. [redacted]

[73] Samsara_000117.

[redacted][74]

90. Samsara does not require its customers to provide any proof of legally sufficient consent and, indeed, [redacted].

91. Samsara's attempt to get written consent through its customers fails legally and factually.

92. First, the text of BIPA is clear that the entity collecting the biometric identifier and biometric information must be the one to obtain consent and it cannot do so derivatively. In contrast to obtaining consent from the "subject" of the biometric collection, where the statute makes it clear that the "subject or the subject's legally authorized representative" may provide consent, the statute does not permit Samsara to obtain consent derivatively through its customers. 740 ILCS 14/15(b).

93. The statutory text indicates that Samsara must be the entity to "inform" the subject of its collection of biometrics, "inform" the subject of its "specific purpose and length of term" for collecting, storing, and using biometrics, and Samsara must "receive" the written release executed by the subject. *Id.*

94. Samsara's policy of deferring completely to its customers is legally deficient.

[74] Samsara_000917.

95. Factually, discovery reveals that [redacted]

96. Specific to Plaintiff, his employer, Lily Transportation, installed Samsara's Dash Cams around August 22, 2021 in the vehicles he operates.[75] Plaintiff was not required to sign any form of consent until December 16, 2021.[76]

97. [redacted][77]

99. [redacted][78]

[75] Deposition of David Karling, Aug. 21, 2023, at 128:19-129:3.
[76] *Id.* at 184:13-16.
[77] Samsara_001186.
[78] Samsara_001174.

[redacted][79]

101. [redacted]

102. Per Plaintiff's experience with Samsara's Dash Cam in his vehicle, [redacted], after Plaintiff had taken numerous other trips, that Lily first asked him to sign a consent form.

103. This example demonstrates precisely why Samsara cannot simply farm out its compliance with BIPA to its customers.

C. Samsara profits from Plaintiff's and Class Members' biometric identifiers and biometric information.

104. BIPA prohibits a private entity, like Samsara, that possesses a biometric identifier or biometric information from "sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

105. Samsara profits from Plaintiff's and Class Members' biometric identifiers and biometric information through the licensing fees charged to its customers. Specifically, [redacted][80]

[79] Samsara_001186.

[80] Samsara's Supplemental Responses to Plaintiff's Third Set of Interrogatories, Sept. 28, 2023, ROG 1.

106. [redacted]

107. Biometric information is a necessary element of Samsara's Camera ID feature. The entire purpose of Camera ID is driver identification. [redacted]

108. Scanning and comparing a face against a database of other faces is no different than social media companies maintaining and searching through a database of customer faces or a technology company selling law enforcement access to its database to find facial matches.

109. Samsara markets the Camera ID feature of its Dash Cams to give it a competitive edge in the marketplace and enhance sales and profits. In so doing, Samsara profits from Plaintiff's and Class Members' biometric information in violation of BIPA.

D. Samsara discloses Plaintiff's and Class Members' biometric identifiers and biometric information without consent.

110. BIPA requires that entities cannot "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure." 740 ILCS 14/15(d)(1).[81]

[81] The other exceptions to disclosure enumerated in the statute (completing a financial transaction, being required to do so by law, or being required by warrant or subpoena) are not applicable here. *See* 740 ILCS 14/15(d)(2)-(4).

111. As detailed above, Camera ID captures Plaintiff's and Class Members' biometric information. That information is disclosed by Samsara to AWS for processing by Rekognition and/or storage through S3.[82]

112. Samsara failed to obtain consent for: (1) its disclosure of biometric information to AWS and (2) its disclosure of biometric information to customers.

113. Specifically, Samsara never directly obtained consent from any truck driver to permit it to disclose their biometric information. Again, Samsara farmed out consent to its customers. This fails legally for the same reasons as it does under Section 15(b).

114. Moreover, the example Illinois Biometric Information Policy that Samsara makes available to its customers is silent about the customer and/or Samsara disclosing Samsara's information to AWS.[83]

115. Thus, the consent forms that Lily belatedly made Plaintiff sign said nothing about AWS or the fact that AWS would receive Plaintiff's biometric information.[84]

116. Thus, Plaintiff and Class Members did not consent to the disclosure of biometric information to AWS because they were never informed of the fact that their biometric information was sent to AWS.

117. Samsara also failed to obtain consent to disclose its biometric information to customers by never obtaining consent directly from drivers.

118. Indeed, most drivers (and even their employers) would have little way of knowing that AWS collects, stores, and uses driver biometric data at all.

[82] Samsara, Security, https://www.samsara.com/legal/security/ (last visited Oct. 16, 2023).
[83] Samsara_000004.
[84] Karling_000092.

119. Few, if any, of Samsara's public-facing sources of information on its facial recognition technology mention that it uses AWS's Rekognition product or that it uploads, stores, and disseminates biometric data using AWS platforms,[85] nor does the sample consent form provided by Samsara to its customers.[86]

120. Through processing and storing driver images sent by Samsara, AWS collected and collects the unique, permanent biometric identifiers and exposed drivers like Plaintiff to irreversible privacy risks. If AWS's database of digitized facial vectors were to fall into the wrong hands, by data breach or otherwise, the individuals to whom these sensitive and immutable biometric identifiers belong could have their identities stolen, among other serious issues.

121. Finally, AWS violates Section 15(d) of BIPA because it discloses, rediscloses, or otherwise disseminates the biometric information of drivers without their consent when it processes drivers' biometric information (through Rekognition or otherwise), stores it on Amazon S3, and then sends that information back to Samsara for use in its Camera ID feature.

E. Samsara is vicariously liable for AWS's violations of BIPA.

1. Samsara exercised actual control over AWS in relation to its use of Rekognition and S3.

122. Alternatively, Samsara violates BIPA through the actions of its agent, AWS.

123. Upon information and belief, AWS acted within the scope of its authority as Samsara's agent when it processed, collected, used, stored, and disseminated biometric

[85] Special Features, https://www.samsara.com/support/privacy/special-features/ (last visited Oct. 16, 2023); Samsara Terms of Service, https://www.samsara.com/legal/platform-terms-of-service (last visited Oct. 16, 2023); Automatic Driver Detection (Camera ID), https://kb.samsara.com/hc/en-us/articles/360042878172-Automatic-Driver-Detection-Camera-ID- (last visited Oct. 16, 2023).

[86] Camera ID Driver Consent, https://kb.samsara.com/hc/en-us/articles/360036848351-Camera-ID-Driver-Consent (last visited Oct. 16, 2023).

information in the ways described above on Samsara's behalf. Upon information and belief, the relationship between Samsara and AWS is governed by a written contract outlining the scope of this authority in which AWS agrees to act as Samsara's agent and at Samsara's direction.[87]

124. Upon information and belief, Samsara had the right to control how AWS processed, collected, used, stored, and disseminated the data Samsara sent to AWS.

125. For example, [redacted][88]

126. Additionally, Samsara controlled the storage by AWS of driver biometric information collected through Camera ID. For instance, [redacted][89]

127. The services that AWS performed on behalf of Samsara benefitted Samsara, in that they allowed Samsara to develop, market, and sell biometric facial recognition software to its customers.

128. Thus, in addition to being directly liable, Samsara is also vicariously liable for BIPA violations caused by the use of Rekognition. Under principles of agency law, AWS through its Rekognition tool functioned as Samsara's agent because it is subject to the actual authority of Samsara. Additionally, the Rekognition tool functioned as Samsara's software agent under principles of agency law.

[87] Samsara has not produced its contract with AWS. This is presently the subject of a pending discovery dispute before the Court. *See* Dkt. 74.

[88] Samsara's Supplemental Response to Plaintiff's Second Set of Interrogatories, Sept. 28, 2023, at ROG 2.

[89] *Id.*

2. Samsara ratified actions taken by AWS vis-à-vis customer data.

129. Samsara knew that the processing, collection, use, storage, and dissemination of driver biometric data by AWS violated BIPA and allowed AWS to continue to perform these actions on its behalf.

130. In the alternative, Samsara was willfully ignorant of AWS's BIPA violations.

131. Samsara has timely manifested its assent to the actions taken by AWS vis-à-vis customer biometric data through its continuing use of Rekognition and S3 to process, collect, store, and disseminate driver's biometric information.

132. AWS has been sued numerous times for its Rekognition product allegedly violating BIPA. For example, in *Rivera v. Amazon Web Services, Inc.*, 2023 WL 4761481 (W.D. Wash. July 26, 2023), the Western District of Washington Court denied AWS's motion to dismiss BIPA claims alleging that the Rekognition product violates Sections 15(a) and (b) of BIPA. In that suit, the plaintiffs allege that Rekognition's product collects their biometrics, indexes them, and possesses their information in violation of BIPA and Rekognition fails to have a publicly available retention schedule. *Id.* Likewise, in *Hogan v. Amazon.com, Inc.*, 2022 WL 952763 (N.D. Ill. Mar. 30, 2022), the plaintiffs sued arguing that their Amazon Photos service used Rekognition to collect their biometrics without consent. There, Judge Leinenweber denied Amazon's motion to dismiss a claim under Section 15(b) and held that the statements in Amazon's Terms of Use did not satisfy BIPA's consent requirements.[90]

133. Samsara did not end its relationship with AWS despite these sustained allegations and thus ratified AWS's collection of biometrics using Rekognition.

[90] In the same order, the Court remanded the plaintiffs' BIPA Sections 15(a) and (c) claims to Illinois state court.

134. Alternatively, ratification is easily presumed based on Samsara's continuing use of AWS products vis-à-vis driver biometric data.

135. Further indicating its assent, at no point did Samsara limit or stop AWS's processing or storage of driver biometric data. Rather, Samsara continues to use AWS for the storage, processing, and dissemination of driver biometric information to this day, including information collected in the State of Illinois in violation of BIPA.

V. Named Plaintiff's Allegations

136. During the relevant time, Plaintiff Karling worked as a driver in Illinois for a commercial customer of Samsara, Lily Transportation.

137. On or around August 22, 2021, Plaintiff Karling's employer installed a Dash Cam, provided by Samsara, in the truck Mr. Karling operates.

138. Plaintiff Karling did and does operate a truck equipped with a Samsara Dash Cam and has done since on or around August 22, 2021.

139. Plaintiff Karling's employer requires him to use Samsara's Dash Cam.

140. Samsara uses its Dash Cam to extract biometric identifiers from Plaintiff Karling's face while he drives and sends them to AWS to be stored through S3. The Dash Cam automatically performs facial recognition to identify him by sending his biometric identifiers to AWS to be processed and compared against his biometric identifiers, which Samsara previously extracted and sent to AWS.

141. Plaintiff Karling never consented, agreed or gave permission—written or otherwise—to Samsara for the collection or storage of his unique biometric identifiers or biometric information.

142. Further, Samsara did not provide Plaintiff Karling with, nor did he ever sign, a written release allowing Samsara to collect or store his unique biometric identifiers or biometric information.

143. The only consent form signed by Plaintiff Karling was offered by his employer, Lily Transportation, on December 16, 2021, almost four months after the Samsara cameras were installed in Plaintiff Karling's cab.

144. Likewise, Samsara did not provide Plaintiff Karling with the requisite statutory disclosures nor an opportunity to prohibit or prevent the collection, storage, or use of his unique biometric identifiers or biometric information.

145. By collecting Plaintiff Karling's unique biometric identifiers or biometric information without his consent, written or otherwise, Samsara invaded Plaintiff Karling's statutorily protected right to privacy in his biometrics.

146. Finally, Samsara did not provide Plaintiff Karling with a retention schedule and/or guidelines for permanently destroying his biometric identifiers and biometric information.

CLASS ALLEGATIONS

147. **Class Definition:** Plaintiff brings this action on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

> All individuals who, while present in the State of Illinois, were subject to Samsara's Camera ID feature.

148. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**. The number of persons within the Class is substantial, "approximately 49,000 drivers employed by Samsara's customers…currently have Camera ID enabled and began a trip in the state of Illinois."[91] It is,

[91] Samsara's Amended Responses to Plaintiff's Amended First Set of Interrogatories, Apr. 7, 2023, ROG 14.

therefore, impractical to join each Class Member, particularly given the relatively modest value of any individual claim. Indeed, Defendant does not contest numerosity. *See* Dkt. 61.

149. **Typicality: Federal Rule of Civil Procedure 23(a)(3)**. Plaintiff's claims are typical of the claims of Class Members in that Plaintiff, like all Class Members, had his biometric identifiers collected, captured, stored, processed, disseminated, disclosed, and redisclosed by Samsara without their consent and in violation of 740 ILCS 14/15(b) & (d). Plaintiff is further typical of the Class in that he was impacted by the lack of publicly available retention schedules for his biometric information, which Samsara failed to make available in violation of 740 ILCS 14/15(a). Finally, Plaintiff is typical of the Class in that Samsara profited off his biometric information in violation of 740 ILCS 14/15(c).

150. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and (b)(3)**. There are well-defined common questions of fact and law that exist as to all Class Members, and that predominate over any questions affecting only individual Class Members. These common legal and factual questions do not vary across Class Members and may be determined without reference to the individual circumstances of any individual. They, include, but are not limited to:

(a) whether Defendant collected or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

(b) whether Defendant properly informed Plaintiff and the Class that it collected, used, and stored Plaintiff's and Class Members' biometric identifiers or biometric information;

(c) whether Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiff's and Class Members' biometric identifiers or biometric information;

(d) whether Defendant developed written policies, 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 Plaintiff's and Class Members' biometric identifiers or biometric information to identify them;

(f) whether Defendant sold, leased, traded, or profited from Plaintiff's and Class Members' biometric identifiers or biometric information; and

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

151. **Adequacy: Federal Rule of Civil Procedure 23(a)(4)**. Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiff and his counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiff is able to fairly and adequately represent and protect the interests of the Class. Neither Plaintiff nor his counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff 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, or to amend the class definition to address any steps that Samsara took.

152. **Superiority**: **Federal Rule of Civil Procedure 23(b)(3)**. A class action is the superior method for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class Members is impracticable. Even if every Class Member 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 Class Member. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with BIPA.

COUNT I
FOR DAMAGES AGAINST SAMSARA

VIOLATION OF 740 ILCS 14/15(A) – FAILURE TO INSTITUTE, MAINTAIN, AND ADHERE TO PUBLICLY AVAILABLE RETENTION SCHEDULE (ON BEHALF OF PLAINTIFF AND THE CLASS)

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

154. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention—and, importantly, deletion—policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS 14/15(a).

155. Samsara failed to comply with these BIPA mandates.

156. Because Samsara is a corporation, it is a "private entity" under BIPA. *See* 740 ILCS 14/10.

157. Plaintiff is an individual who had his "biometric identifiers" captured and/or collected by Samsara, as explained in detail in above. *See* 740 ILCS 14/10.

158. Plaintiff's biometric identifiers were used to identify Plaintiff and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

159. Samsara 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).

160. Samsara's purported retention schedule and policy was deficient for the reasons stated above and the Court previously held in its motion to dismiss order that it "says nothing about destruction guidelines." Dkt. 25 at 11.

161. [redacted]

162. Thus, Samsara lacked retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and have not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

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

COUNT II
FOR DAMAGES AGAINST SAMSARA

VIOLATION OF 740 ILCS 14/15(B) – FAILURE TO OBTAIN INFORMED WRITTEN CONSENT AND RELEASE BEFORE OBTAINING BIOMETRIC IDENTIFIERS OR INFORMATION
(ON BEHALF OF PLAINTIFF AND THE CLASS)

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

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

166. Samsara failed to comply with these BIPA mandates.

167. Because Samsara is a corporation, it is a "private entity" under BIPA. *See* 740 ILCS 14/10.

168. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected and/or captured by Samsara, as explained in detail above. *See* 740 ILCS 14/10.

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

170. Samsara systematically and automatically collected, captured, used, and stored Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

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

172. By collecting, capturing, storing, and/or using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Samsara violated Plaintiff's and the Class's rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

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

COUNT III
FOR DAMAGES AGAINST SAMSARA

VIOLATION OF 740 ILCS 14/15(C) – BY PROFITING FROM PLAINTIFF'S AND CLASS MEMBERS' BIOMETRIC IDENTIFIERS OR INFORMATION (ON BEHALF OF PLAINTIFF AND THE CLASS)

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

175. BIPA prohibits a private entity from "sell[ing], leas[ing], trad[ing], or otherwise profit[ing] from a person's or a customer's biometric identifier or biometric information." *See* 740 ILCS 14/15(c).

176. Samsara fail to comply with this BIPA mandate.

177. Because Samsara is a corporation, it is a "private entity" under BIPA. *See* 740 ILCS § 14/10.

178. Plaintiff is an individual who had his "biometric identifiers" captured and/or collected by Samsara, as explained in detail in above. *See* 740 ILCS 14/10.

179. Plaintiff's biometric identifiers were used to identify Plaintiff and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

180. Samsara possesses Plaintiff's and Class Members' biometric identifiers and/or biometric information.

181. Samsara profits from Plaintiff's and Class Members' biometric identifiers and/or biometric information through the licensing fees it charges its customers for its cameras.

182. By profiting from Plaintiff's and Class Members' biometric identifiers and/or biometric information, Samsara violated Plaintiff's and the Class's rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS 14/10(c).

183. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Samsara to comply with BIPA's requirements for the collection, captures, storage, use and dissemination of biometric identifiers and biometric information as described herein pursuant to 740 ILCS 14/20(4); (3) liquidated damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, liquidated

damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT IV
FOR DAMAGES AGAINST SAMSARA

VIOLATION OF 740 ILCS 14/15(D) – BY DISCLOSING AND REDISCLOSING PLAINTIFF'S AND CLASS MEMBERS' BIOMETRIC IDENTIFIERS OR INFORMATION
(ON BEHALF OF PLAINTIFF AND THE CLASS)

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

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

186. Samsara fail to comply with this BIPA mandate.

187. Because Samsara is a corporation, it is a "private entity" under BIPA. *See* 740 ILCS 14/10.

188. Plaintiff is an individual who had his "biometric identifiers" captured and/or collected by Samsara, as explained in detail in above. *See* 740 ILCS 14/10.

189. Plaintiff's biometric identifiers were used to identify Plaintiff and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

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

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

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

PRAYER FOR RELIEF

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

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing his counsel as Class Counsel;

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

C. Awarding liquidated 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, liquidated damages of $1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if the Court finds that Samsara'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 Samsara to collect, store, and use biometric identifiers and/or biometric information in compliance with BIPA;

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

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

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

Dated: August 30, 2024

Respectfully submitted,

DAVID KARLING,
individually and on behalf of all
others similarly situated

/s/ Sean A. Petterson

Gary M. Klinger (IL Bar No. 6303726)
Alexander E. Wolf
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
866.252.0878
gklinger@milberg.com

Jason L. Lichtman (IL Bar #6290052)
Sean A. Petterson (*pro hac vice*)
Muriel Kenfield-Kelleher (IL Bar #6339202)
LIEFF CABRASER HEIMANN & BERNSTEIN LLP
250 Hudson Street, 8th Floor
New York, New York 10013
212.355.9500

Attorneys for Plaintiff and the Proposed Class