

2. Plaintiff opened a Hinge account within the last five years.

3. As part of signing up, and/or gaining access to his Hinge account, Plaintiff was asked to allow Defendant to collect his facial geometry, *i.e.*, his biometric information in order to have the Photo Verification feature on their profile.

4. The Photo Verification feature on a Hinge profile account allows the user to obtain a verification badge on their profile that shows their uploaded photos are an accurate portrayal of the user and are not an instance of false identification.

5. This Photo Verification process has a two-step process. First, the user takes a video of themselves referred to as a “Liveness Check” to be sure that the verification video uploaded was from a real, live person and not digitally manipulated or altered. Second, a “3D Face Authentication” is used that scans and detects the users face in their uploaded profile pictures as well as the “Liveness Check” video, creating a unique number also known as a “template” using facial geometry scanning software to verify that all the facial features are the same and thus the individual who uploaded the video is the same as the individual in the uploaded profile pictures.

6. Facial geometry scans are unique, permanent biometric identifiers associated with each user that cannot be changed or replaced if stolen or compromised. Hinge’s unlawful collection, obtainment, storage, and use of its users' biometric data exposes them to serious and irreversible privacy risks. For example, if Hinge, or their third-party affiliates’ databases containing facial geometry scans or other sensitive, proprietary biometric data are hacked, breached, or otherwise exposed, Hinge users have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

7. Hinge collects, stores, possesses, otherwise obtains, uses, and disseminates its users' biometric data to, amongst other things, further enhance Hinge and its online dating platform.

8. The Illinois legislature enacted BIPA to protect residents' privacy interests in their biometric data. *See Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 963 (N.D. Ill. 2020), citing *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, 432 Ill. Dec. 654, 129 N.E.3d 1197, 1199 (2019).

9. Courts analogize an individual's privacy interest in their unique biometric data to their interest in protecting their private domain from invasion, such as from trespass. *See Bryant v. Compass Group USA, Inc.*, 958 F.3d 617, 624 (7th Cir. 2020), as amended on denial of reh'g and reh'g *en banc*, (June 30, 2020) and opinion amended on denial of reh'g *en banc*, 2020 U.S. App. LEXIS 20468, 2020 WL 6534581 (7th Cir. 2020).

10. In recognition of these concerns over the security of individuals' biometrics, the Illinois Legislature enacted the BIPA, which provides, *inter alia*, that a private entity like Match Group, LLC may not obtain and/or possess an individual's biometrics unless it: (1) informs that person in writing that biometric identifiers or information will be collected or stored; (2) informs that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, stored and used; (3) receives a written release from the person for the collection of his or her biometric identifiers or information; and (4) publishes publicly-available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information. 740 ILCS 14/15(a)-(b).

11. The Illinois Legislature has found 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.*

12. Specifically, upon information and belief, Hinge has created, collected, disseminated, and stored thousands of “face templates” (highly detailed geometric maps of the face) from countless Illinois residents whose selfies were collected by Hinge.

13. Each face template that Hinge extracts are unique to a particular individual in the same way that a fingerprint or voiceprint identifies an individual.

14. Hinge is a “private entity” as that term is broadly defined by BIPA and is subject to all requirements of BIPA. *See* 740 ILCS § 14/10.

15. Plaintiff is informed and believes, and based thereon alleges, that at all relevant times mentioned herein, Defendant acted as agents, employees, supervisors, partners, conspirators, servants and/or joint venturers of each other, and in doing the acts hereafter alleged, were acting within the course, scope, and authority of such agency, employment, partnership, conspiracy, enterprise and/or joint venture, and with the express and/or implied permission, knowledge, consent, authorization and ratification of their co-defendants.

JURISDICTION

16. This is a Class Action Complaint for violations of the Illinois Biometric Information Privacy Act (740 ILCS § 14/1 *et seq.*) brought pursuant to 735 ILCS §§ 5/2-801, 2-802 seeking statutory damages.

17. At all relevant times, Plaintiff and the proposed Class are residents of the state of Illinois and the violations of BIPA as detailed herein occurred while Plaintiff and the proposed Class were in the state of Illinois.

18. Hinge markets directly to Illinois residents and does substantial business with users located in and residing within the State of Illinois.

19. Hinge's marketing efforts include, but are not limited to, Facebook ads, Instagram ads, and other social media marketing campaigns targeted specifically at individuals residing within the City of Chicago and State of Illinois.

20. At all relevant times, Match Group, LLC is a Delaware corporation with its principal place of business located in Dallas, Texas.

FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS

24. Plaintiff realleges and incorporates by reference all allegations in all preceding paragraphs.

25. Plaintiff opened a Hinge account within the five years immediately preceding the filing of this Complaint.

26. As part of signing up, and/or gaining access to his Hinge account, Plaintiff was prompted to upload a real time portrait of his face in addition to other identification information such as Plaintiff's legal name and date of birth.

27. Hinge then scanned Plaintiff's verification photographs, creating a biometric template of Plaintiff's face and biometric identifiers, and compared Plaintiff's biometric identifiers to the photographs which Plaintiff posted on his Hinge profile in order to verify Plaintiff's identity.

28. In other words, Hinge collected and retained biometric information for the purpose of verifying Plaintiff's identity.

29. At the time of collecting and retaining Plaintiff's biometric information Hinge had no written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric information when the initial purpose for collecting or obtaining such biometric information has been satisfied or within 3 years of the individual's last interaction with Hinge, whichever occurs first.

30. Ostensibly, the purpose of Hinge's collection of Plaintiff's facial geometry was to verify Plaintiff's identity.

31. As such, Plaintiff's facial geometry should have been permanently destroyed by Defendant following the verification of Plaintiff's identity.

32. However, Hinge failed to permanently destroy Plaintiff's facial geometry following the verification of Plaintiff's identity and instead retained Plaintiff's biometric information and disseminated it to a third-party processor.

33. As such, Hinge's retention of Plaintiff's biometric information was unlawful and in violation of 740 ILCS § 14/15(a).

34. Hinge did not inform Plaintiff in writing that it was collecting or storing her biometric information.

35. Instead, Hinge simply instructed Plaintiff to upload her "selfie" photograph as part of the overall account verification process.

36. In fact, Hinge made no mention of biometric information, collection of biometric information, or storage of biometric information.

37. Moreover, Hinge did not inform Plaintiff in writing of the specific purpose and length of term for which her biometric information was being collected, stored, and used.

38. Hinge collected, stored, and used Plaintiff's biometric information without ever receiving a written release executed by Plaintiff in which he consented to or authorized Defendant to do same.

39. Additionally, Hinge disclosed, redisclosed, or otherwise disseminated Plaintiff's biometric information (1) without Plaintiff's consent; (2) without Plaintiff's authorization to complete a financial transaction requested or authorized by Plaintiff; (3) without being required by State or federal law or municipal ordinance; or (4) without being required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

40. Upon information and belief, Hinge disclosed, redisclosed, or otherwise disseminated Plaintiff's biometric information to numerous third-party service providers for Hinge's business purposes, including but not limited to, third party providers that provide business services to Hinge, third-party service providers that provide professional services to Hinge, and third-party service providers that provide technical support functions to Hinge.

41. Hinge's collection and retention of biometric information as described herein is not unique to Plaintiff and is instead part of Hinge's policies and procedures which Hinge applies to all its users, including the Class Members.

CLASS DEFINITIONS AND ALLEGATIONS

42. Plaintiff realleges and incorporates by reference all allegations in all preceding paragraphs.

43. Plaintiff brings Claims for Relief in violation of BIPA as a class action under 735 ILCS §§ 5/2-801 and 2-802. Plaintiff brings these claims on behalf of himself and all members of the following Class:

All Illinois residents who had their biometric information collected by Match Group, LLC while using the application Hinge at any point in the five (5) years preceding the filing of this Complaint (the “Class Members”).

44. In the alternative, and for the convenience of this Court and the parties, Plaintiff may seek to certify other subclasses at the time the motion for class certification is filed.

45. **Numerosity:** The Class Members are so numerous that joinder of all members is impracticable. Plaintiff is informed and believes that there are more than 1,000 people who satisfy the definition of the Class.

46. **Existence of Common Questions of Law and Fact:** Common questions of law and fact exist as to Plaintiff and the Class Members including, but not limited to, the following:

a. Whether Hinge possessed Plaintiff’s and the Class Members’ biometric identifiers or biometric information without first developing 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 Hinge, whichever occurs first.

b. Whether Hinge collected, captured, purchased, received through trade, or otherwise obtained Plaintiff’s and the Class Members’ biometric identifiers or biometric information, without first: (1) informing Plaintiff and the Class Members in writing that a biometric identifier or biometric information is being collected or stored; (2) informing Plaintiff and the Class Members in writing of the specific purpose and length of term for which their biometric identifiers or biometric information was being collected, stored, and used; and (3) receiving a written release executed by Plaintiff and the Class Members

c. Whether Hinge disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class Members' biometric identifiers or biometric information (1) without Plaintiff's and the Class Members' consent; (2) without Plaintiff's and the Class Members' authorization to complete a financial transaction requested or authorized by Plaintiff and the Class Members; (3) without being required by State or federal law or municipal ordinance; or (4) without being required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

d. The damages sustained and the proper monetary amounts recoverable by Plaintiff and the Class Members.

47. **Adequacy:** Plaintiff's claims are typical of the Class Members' claims. Plaintiff, like the Class Members, had her biometric identifiers and biometric information collected, retained or otherwise possessed by Hinge without Hinge's adherence to the requirements of BIPA as detailed herein. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff has retained counsel competent and experienced in complex class actions.

48. **Predominance and Superiority of Class Action:** Class certification is appropriate because questions of law and fact common to the Class Members predominate over questions affecting only individual members of the class, and because a class action is superior to other available methods for the fair and efficient adjudication of this litigation. Hinge's common and uniform policies and practices illegally deprived Plaintiff and the Class Members of the privacy protections which BIPA seeks to ensure; thus, making the question of liability and damages much more manageable and efficient to resolve in a class action, compared to hundreds of individual trials. The damages suffered by individual Class Members are small compared to the expense and burden of individual prosecution. In addition, class certification is superior because

it will obviate the need for unduly duplicative litigation that might result in inconsistent judgments about Hinge's practices.

COUNT ONE: VIOLATION OF 740 ILCS § 14/15(a)

(Brought by Plaintiff on behalf of himself and the Class Members against Defendant)

49. Plaintiff realleges and incorporates by reference all allegations in all preceding paragraphs.

50. 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. 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).

51. Defendant collected Plaintiff's and the Class Members facial geometry scans and created biometric templates of the Plaintiff's and the Class Members' faces which qualifies as biometric information as defined by BIPA.

52. At all relevant times, Defendant had no written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric information when the initial purpose for collecting or obtaining such biometric information has been satisfied or within 3 years of the individual's last interaction with Defendant, whichever occurs first.

53. Ostensibly, the purpose of Defendant's collection of Plaintiff's and the Class Members' facial geometry was to verify Plaintiff's and the Class Members' identities prior to

verifying a Hinge account in their names and the purpose of Defendant's collection Plaintiff's and the Class Members' geometric facial scans was to verify Plaintiff's and the Class Members' identities when they logged into the Hinge mobile app.

54. As such, Plaintiff's and the Class Members' facial geometry should have been permanently destroyed by Defendant following the verification of their Hinge accounts.

55. However, Defendant failed to permanently destroy Plaintiff's and the Class Members' biometric information following the verification of their Hinge accounts and instead retained Plaintiff's and the Class Members' biometric information.

56. As such, Defendant's retention of Plaintiff's and the Class Members' biometric information was unlawful and in violation of 740 ILCS § 14/15(a).

COUNT TWO: VIOLATION OF 740 ILCS § 14/15(b)

(Brought by Plaintiff on behalf of himself and the Class Members against Defendant)

57. Plaintiff realleges and incorporates by reference all allegations in all preceding paragraphs.

58. No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs 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) 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).

59. Defendant did not inform Plaintiff and the Class Members in writing that Defendant was collecting or storing their biometric information.

60. Instead, Defendant simply instructed Plaintiff and the Class Members to upload their “selfies” as part of the overall account verification process.

61. In fact, Defendant made no mention of biometric information, collection of biometric information, or storage of biometric information.

62. Moreover, Defendant did not inform Plaintiff and the Class Members in writing of the specific purpose and length of term for which their biometric information was being collected, stored, and used.

63. Defendant collected, stored, and used Plaintiff’s and the Class Members’ biometric information without ever receiving a written release executed by Plaintiff and the Class Members which would consent to or authorize Defendant to do same.

64. As such, Defendant’s collection of Plaintiff’s and the Class Members’ biometric information was unlawful and in violation of 740 ILCS § 14/15(c).

COUNT THREE: VIOLATION OF 740 ILCS § 14/15(d)

(Brought by Plaintiff on behalf of himself and the Class Members against Defendant)

65. Plaintiff realleges and incorporates by reference all allegations in all preceding paragraphs.

66. No private entity in possession of a biometric identifier or biometric information may 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;
- (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction. 740 ILCS § 14/15(d).

67. While discovery will ascertain all of the ways in which Defendant disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class Members' biometric information, Defendant disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class Members' biometric information to numerous third party service providers for Defendant's business purposes, including but not limited to, third party providers that provide business services to Defendant, third party service providers that provide professional services to Defendant, and third party service providers that provide technical support functions to Defendant.

68. Defendant's disclosures, redisclosures, or otherwise disseminating of Plaintiff's and the Class Members' biometric information was unlawful and in violation of 740 ILCS § 14/15(d).

PRAYER FOR RELIEF

WHEREFORE, individually, and on behalf of the Class Members, Plaintiff prays for: (1) certification of this case as a class action appointing the undersigned counsel as class counsel; (2) a declaration that Defendant has violated BIPA, 740 ILCS 14/1 *et seq.*; (3) statutory damages of \$5,000.00 for each intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000.00 per violation pursuant to 740 ILCS 14/20(1) in the event the court finds that Defendant's violations of BIPA were not willful; (4) reasonable attorneys' fees and costs and other litigation expense pursuant to 740 ILCS 14/20(3); (5) actual damages; and (6) for any other relief the Court deems appropriate.

Dated: February 3, 2024

Respectfully submitted,

FRADIN LAW

By: /s/ Michael L. Fradin

Michael L. Fradin, Esq.
8 N. Court St. Suite 403
Athens, Ohio 45701
Telephone: 847-986-5889
Facsimile: 847-673-1228
Email: mike@fradinlaw.com

SIMON LAW CO.

By: /s/ James L. Simon

James L. Simon (pro hac vice forthcoming)
Simon Law Co.
5000 Rockside Road
Liberty Plaza – Suite 520
Independence, OH 44131
Telephone: (216) 816-8696
Email: james@simonsayspay.com