UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

KATRINA BERGER, individually and on behalf of herself and all others similarly situated,

Plaintiff,

v.

MATCH GROUP, LLC d/b/a MATCH.COM,

Defendant.

Case No. _____

CLASS ACTION

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Katrina Berger (the "Plaintiff"), on behalf of herself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against the above-captioned Defendant, Match Group, LLC (the "Defendant" or "Match") upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

I. NATURE OF THE ACTION

1. Modern romance, since the dawn of the smartphone, has changed since the days of speed dating and meeting someone serendipitously. Today, one of the most popular ways for two single people to meet each other is through a social referral service, more commonly known as a dating application. Dating applications match profiles of interested singles so that they have the opportunity to meet and potentially enter into a relationship with each other.

2. The largest such dating application provider is called Match.com, the Defendant in this Action, who maintains over 40 dating applications - including "Tinder," which is the dating application used by Plaintiff Berger.

3. Tinder users put a substantial amount of trust into Tinder, anticipating a reasonable expectation of privacy in a highly private situation – dating. And yet, Tinder violates this trust as Tinder collects a vast amount of consumer data, including biometric information, which is highly personal and sensitive. Tinder not only collects this data, but shares it with third parties.

4. As such, Plaintiff Berger brings this action on behalf of herself and all others similarly situated to vindicate their privacy rights under New York state statutes for the collection of facial recognition data through Defendant Match's dating application(s). Plaintiff Berger seeks statutory damages under GBL 394-c of $50 per violation for each of the tens of thousands of

consumers (if not more) in New York who used one of Match's dating applications which collect biometric identifiers (i.e. Tinder) and/or PII, disgorgement of profits, injunctive relief ending the practices of collecting biometrics and sharing said biometrics and/or PII on all of Match's dating applications both currently and into the future, and reasonable attorneys' fees and costs.

II. JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, as: (1) there are over 100 members of the putative class, (2) damages exceed $5,000,000, and (3) one plaintiff is of a different state than one defendant - namely, Plaintiff Berger is a New York resident whereas Defendant Match is headquartered in Texas.

6. This Court has personal jurisdiction over the Defendant because the Defendant has violated the compelling privacy interests of the Plaintiff and members of the Class in this District. Additionally Defendant has purposeful minimum contacts with this District and directs advertising, marketing, and other commerce into this District such that exercising personal jurisdiction over the Defendant would not upset traditional notions of fair play and substantial justice.

7. This Court has is the proper venue for this Action, as the Plaintiff is located in this District, consumers have been harmed in this District, and the Defendant does business and transacts in commerce in this District.

III. PARTIES

Plaintiff Katrina Berger

8. Plaintiff Katrina Berger is a New York resident who is a consumer that uses Defendant Match's dating application(s).

9. Plaintiff Berger's biometric information was collected and shared to unauthorized parties after she uploaded her image for Photo Verification onto Defendant's Tinder application. As such, Plaintiff Berger has been harmed by way of Defendant's data collection and data practices.

Defendant Match Group, LLC

10. Defendant Match Group, LLC is a Texas-based limited liability company with one sole member, Match Group Holdings II, LLC. Match Group Holdings II, LLC has one member as well, Match Group Holdings I, LLC. Match Group Holdings I, LLC has one member as well, Match Group, Inc.

IV. FACTUAL ALLEGATIONS

a. Defendant's Business

11. Match is a monopoly over the dating application market, with over 40 dating applications including the first most popular dating application, Tinder, as well as other popular dating applications including Hinge, Match, and OKCupid. Consumers have little choice, if they wish to enter the dating application space, but to use a Match dating application due to the market share of Match and the fact that the pool of eligible singles would be difficult to find elsewhere other than a Match dating application.

b. The Sensitivity of Biometric Identifier Information

12. As such, a reasonable consumer would submit to the requests of Match in order to be able to continue to seek romance on one of their dating applications.

13. One such request is to provide an extensive trove of personally identifiable information, including biometric identifier information. This is a difficult request to make and one that requires trust between the Defendant and its consumers - including Plaintiff Berger both

because of the highly private and personal nature of dating itself as well as the private nature of the personally identifiable information sought by the Defendant in order to use their dating application(s).

14. Facial recognition data, and biometric information more generally, is highly sensitive personally identifiable information. Biometric identifiers are permanently identifiable features of a person's facial template, fingerprints, and other identifiers which cannot be altered.

15. There are two main classes of biometrics data that can be collected from individuals: (1) behavioral characteristics and (2) physiological characteristics.[1] Behavioral characteristics concern the behavior of an individual, while physiological characteristics concern the shape or composition of the individual's body. Behavioral biometrics include an individual's keystroke, signature, and voice recognition.[2] Physiological biometrics include facial recognition, fingerprint scanning, hand geometry, iris scanning, and DNA.[3] Facial recognition systems use an individual's unchangeable physiological information, such as facial structure, eye color, size, and shape.[4]

---

[1] Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. MARSHALL L. REV. 589, 589–92 (2018) (citing Margaret Rouse, Biometrics, www.searchsecurity.techtarget.com/definition/biometrics; *see* generally What is Biometrics?, IDEMIA, www.morpho.com/en/biometrics (referring to biometrics as all processes used to recognize, authenticate, and identify persons based on certain physical or behavioral characteristics. The characteristics are universal, unique, invariable, recordable, and measurable)) (last visited July 22, 2021).

[2] Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. MARSHALL L. REV. 589, 589–92 (2018) (citing Margaret Rouse, Biometrics, www.searchsecurity.techtarget.com/definition/biometrics; *see* generally What is Biometrics?, IDEMIA, www.morpho.com/en/biometrics (referring to biometrics as all processes used to recognize, authenticate, and identify persons based on certain physical or behavioral characteristics. The characteristics are universal, unique, invariable, recordable, and measurable)) (last visited July 22, 2021).

[3] Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. MARSHALL L. REV. 589, 589–92 (2018) (citing Margaret Rouse, Biometrics, www.searchsecurity.techtarget.com/definition/biometrics; *see* generally What is Biometrics?, IDEMIA, www.morpho.com/en/biometrics (referring to biometrics as all processes used to recognize, authenticate, and identify persons based on certain physical or behavioral characteristics. The characteristics are universal, unique, invariable, recordable, and measurable)) (last visited July 22, 2021).

[4] Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. MARSHALL L. REV. 589, 589–92 (2018).

16. Biometric identifiers come in a variety of forms, including fingerprints, palm prints, iris/retinal scans, and scans of the facial geometry (facial recognition), which are unique to each person. There is a critical need for protecting and securing biometric identifiers because biometric identifiers:

- Create a specific link between an individual and a data record;
- Can be used to create fake digital identities for fraudulent purposes;
- Create a form of identification which is not exchangeable[5]; and,
- Are immutable, and, if compromised by, for example, hacking, the biometric identifiers cannot be changed.

17. Consumer businesses, like Defendant, can use biometrics to identify consumers and link data to that consumer, including linking a consumer's biometric identifier to methods of payment, such as their credit cards and debit cards. The result is the creation of a vast repository of information (consumer purchasing history, purchasing habits, medical history for services paid with that credit card, etc.) that is tied to customer biometric information.

18. "Verification and identification are the two ways in which an individual's identity can be determined using biometric technology. Verification confirms that a person is indeed who they claim to be and performs a one-to-one comparison of the individual's [biometric] sample with a stored reference template. Identification, on the other hand, performs a one-to-many comparison to confirm an individual's identity. The identification process compares the individual's [] sample against all the reference templates stored on file. An individual is positively identified if the individual's [] image matches any of the stored templates."

[5] https://www.miteksystems.com/blog/looking-ahead-7-reasons-why-biometric-security-is-important-for-digital-identity (last accessed July 11, 2021).

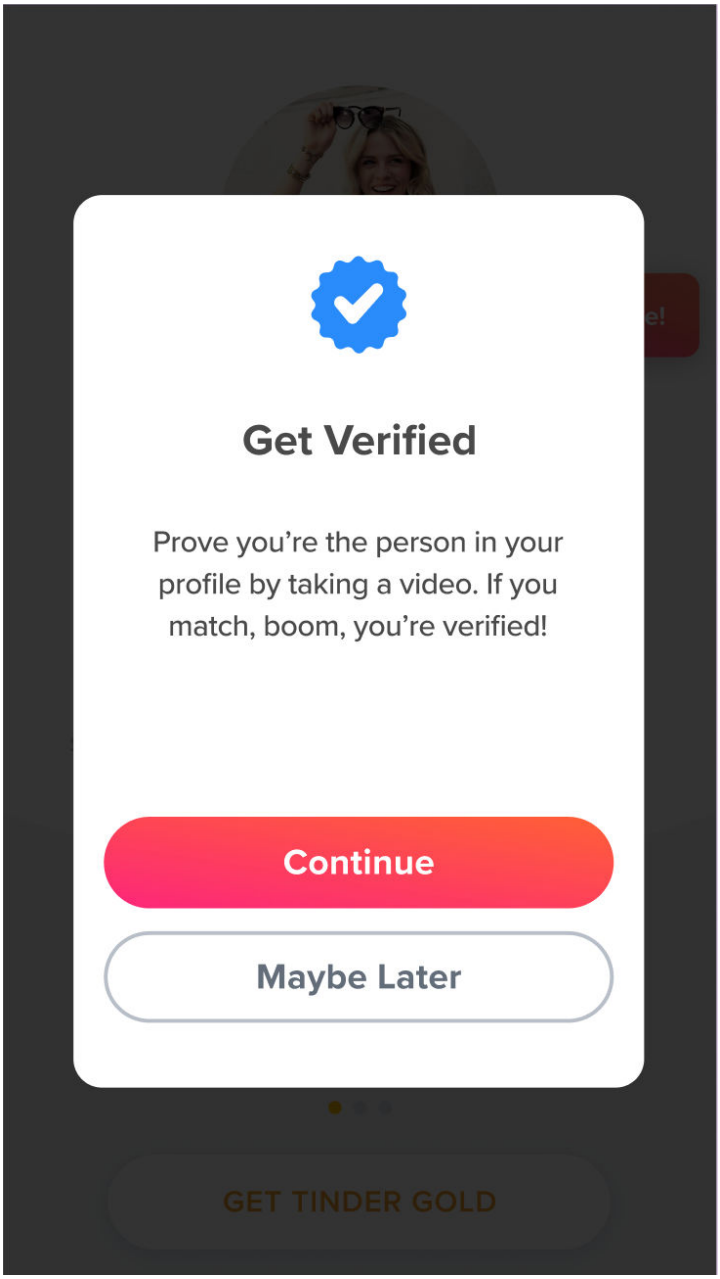
19. Legislatures have correctly identified that the privacy rights tied to biometric identifiers is a worthy right warranting statutory protection. As such, state legislatures and city councils across the country have either passed or are considering passing biometric privacy statutes in order to protect the privacy rights of their constituents.

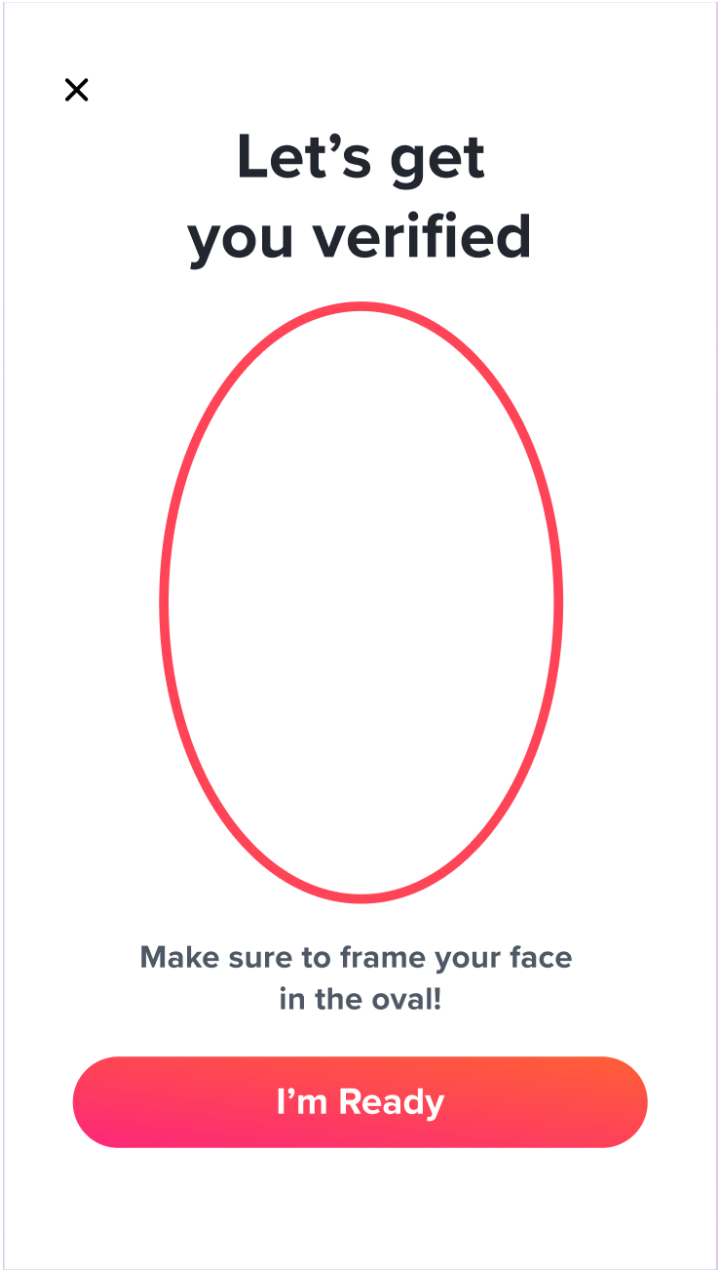
c. Defendant Collects and Shares Biometric Information

20. Defendant collects biometric information — Defendant admits as such in numerous articles, on their own website, and in their privacy policy.

21. Tinder states on their website, "[p]hoto verification provides an opportunity for you to show potential matches you're really you. To get verified, you'll submit a short video selfie that we'll compare to your profile photos. We use a combo of trusty humans and facial recognition technology to compare facial geometry in the selfies you submit and in your profile pics."

22. The submission pages with the Tinder application look as follows:


Get Verified
Prove you're the person in your profile by taking a video. If you match, boom, you're verified!
Continue
Maybe Later
GET TINDER GOLD



23. According to Defendant, "[y]ou will receive 'Photo Verified' status if the person in your video selfie passes both the Liveness Check and the 3D Face Authentication steps. The Liveness Check scans the face in your video and helps us confirm that the video was taken by a real, live person… 3D Face Authentication detects your face in your video selfie and your profile photos, and extracts facial geometries using facial recognition technology to create a unique

number or geometry template. These templates are used to check whether the person in your video selfie is the same person as in your photos."

24. The reason that the Defendant allegedly collects this information, according to Defendant, is to combat fake profiles. One of the main issues with dating applications is the creation and use of fake profiles - which are profiles created by perpetrators with nefarious intentions who often are seeking to commit fraud or other harm to innocent single people. Fake profiles often are populated with pictures of unassuming victims scraped from the internet in order make the fake profile seem legitimate. Tinder combats the proliferation of these fake profiles by using facial recognition to match the profile's creator with the pictures that that creator is using on the profile itself. This verification process, called Photo Verification, consists of users uploading a video of themselves so that facial recognition can confirm they are who they say they are.

25. Defendant not only collects this information but also reshares it with unauthorized third parties contrary to the privacy rights protected by statute and contrary to the privacy rights that the Defendant claims to support by way of its Privacy Policy. This is a breach of consumer trust, violates consumers' privacy rights, and is a flagrant disregard for the sensitivity consumers' of biometric information.

26. The California Privacy Rights page – which a New York (or non-California) user would not be expected to review -- with respect to biometrics, states that biometric information is disclosed to "[v]endors and professional services organizations who assist us in relation to the operation of the feature."

27. There are other, less intrusive ways to verify that users are who they say they are without collecting biometric information – and there are certainly ways of doing so without sharing said biometric information.

d. Defendant Also Collects and Shares a Trove of Other Highly Personal Information

28. In addition to biometric information, the Defendant also collects other highly personally identifiable information ("PII"), which, by way of its California privacy rights page, which, again, New York and non-California users would not have reason to reason to review, admits to sharing said information with anyone from product vendors to professional services organizations to "joint marketing partners." This information includes but is not limited to:

a. Identifiers such as a real name, alias, postal address, unique personal identifier (such as a device identifier; cookies, beacons, pixel tags, mobile ad identifiers and similar technology; customer number, unique pseudonym, or user alias; telephone number and other forms of persistent or probabilistic identifiers), online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, and other similar identifiers;

b. Signature, physical characteristics or description, state identification card number, education, bank account number, credit card number, debit card number, other financial information, and medical information; and,

c. Characteristics of protected classifications under California or federal law, such as race, color, national origin, religion, age, sex, gender, gender identity, gender expression, sexual orientation, marital status, medical condition, disability, citizenship status, and military and veteran status.

29. Additionally, the Defendant collects the following information which is shared with vendors and professional services organizations for "commercial purposes," including: internet and other electronic network activity information, including, but not limited to, browsing history,

search history, and information regarding your interaction with websites, applications or advertisements.

30. Defendant's dating application collects a massive amount of PII and shares that PII with parties that any person, including the Plaintiff and members of the Class, on a dating application would find highly offensive. Plaintiff and the members of the Class not only have no control over who their data is shared with, but have no idea who the end user of their PII ultimately is, the purposes for which that data is being collected and how it will be used.

31. PII has value – which is why data breaches and ransomware attacks have become so prevalent; that information, if the hacker is successful, is then taken, repackaged and sold on the dark web.

32. By sharing PII with unknown third parties, Defendant not only deprives Plaintiff and Class members of the value of their PII, but then passes along that PII to parties who could use it for their own benefit and, potentially, in nefarious ways.

V. CLASS ALLEGATIONS

33. Plaintiff seeks to certify a class consisting of consumers who fall under the following definition ("Class Definition" or, the "Class"):

> **Nationwide Class.** All users across the United States of Defendant's dating applications who had their biometric identifying information and/or PII collected by the Defendant during the applicable statute of limitations.
>
> **New York Class.** All users across the state of New York of Defendant's dating applications who had their biometric identifying information and/or PII collected by the Defendant during the applicable statute of limitations.

34. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives,

attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

35. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

36. **Numerosity.** The members of the Classes are so numerous that individual joinder of all Class Members is impracticable. On information and belief, Class Members number in the thousands to millions. The precise number or identification of members of the Classes are presently unknown to Plaintiff but may be ascertained from Defendants' books and records. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

37. **Commonality and Predominance.** Common questions of law and fact exist as to all members of the Classes, which predominate over any questions affecting individual members of the Classes. These common questions of law or fact include, but are not limited to, the following:

i. Whether Defendant collected biometric identifier information from customers;

ii. Whether Defendant collected PII from customers;

iii. Whether biometric identifier information and other PII is considered to be sensitive personal information under GBL 394-c;

iv. Whether Defendant shared biometric identifier information and other PII;

v. Whether Plaintiff and the Class are entitled to damages, statutory damages, and/or injunctive relief.

38. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

39. **Typicality.** Plaintiff's claims are typical of the claims of the other Class Members because, among other things, all such claims arise out of the same wrongful course of conduct engaged in by Defendant in violation of law as complained of herein. Further, the damages of each Class Member were caused directly by Defendant's wrongful conduct in violation of the law as alleged herein.

40. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and Plaintiff's interests do not conflict with the interests of the Class Members she seeks to represent. Plaintiff has retained counsel competent and experienced in complex commercial and class action litigation. Plaintiff and her counsel intend to prosecute this action vigorously for the benefit of all Class Members. Accordingly, the interests of the Class Members will be fairly and adequately protected by Plaintiff and her counsel.

41. **Superiority.** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not.

Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I
Violations of Gen. Bus. L. § 394-c
("GBL 394-c')
On Behalf of the New York State Class

42. Plaintiff incorporates all of the foregoing paragraphs as if fully restated herein.

43. Under GBL 394-c, a "social referral service" shall include any service for a fee providing matching of members of the opposite sex, by use of a computer or any other means, for the purpose of dating and general social contact.

44. Plaintiff and the members of the Class are consumers for a social referral service under the statute – namely, they are consumers of Defendant Match's dating application(s).

45. GBL 394-c provides certain rights for consumers of social referral services and allows a consumer to bring an action in Court, like this Action, if those rights are violated.

46. In this Action, Plaintiff Berger and the Class Members have had the following rights violated, which include but are not limited to the following:

a. "Every contract for social referral service shall provide that the seller will not without prior written consent of the purchaser sell, assign or otherwise transfer for business or any other purpose to any person any information of a personal or private nature acquire from the purchaser directly or indirectly including but not limited to… photographs and background information."

i. Defendant violates this provision of the statute by collecting PII and facial recognition data through the Photo Verification process and then by sharing that information with other parties, vendors, and other business partners.

b. "If any provision of the social referral service contract is violated, you have the right to bring a court action against the provider which has violated the contract."

i. Defendant violates this provision of the statute by making representations about privacy representations in their Privacy Policy which are blatantly untrue – namely, that they value privacy, when, in reality, they collect and share sensitive biometric identifier information and/or PII with unknown third parties.

47. Any person who has been injured by reason of a violation of the foregoing section(s) may bring an action in his or her own name to enjoin such violation, an action to recover his or her actual damages or fifty dollars, whichever is greater, or both such actions.

48. Plaintiff Berger and the members of the Class have been harmed and move to bring this Action in court to recover all available damages inclusive of statutory damages and injunctive relief.

COUNT II
Unjust Enrichment
On Behalf of the Nationwide Class

49. Plaintiff incorporates all of the foregoing paragraphs as if fully restated herein.

50. Defendant's collection, retention, and sharing/selling of biometric information and/or PII allows the Defendant to retain profits which would be unjust to allow the Defendant to retain. Biometric information and PII is extremely sensitive – and therefore extremely valuable.

Thus, Plaintiff and the Class conferred a benefit onto the Defendant by providing their biometric information and/or PII to the Defendant.

51. Under the principles of equity and good conscience, allowing Defendant to continue to profit off its illegal treatment of this data would be improper and harms Plaintiff and members of the Class.

VII. PRAYER FOR RELIEF

52. **WHEREFORE,** Plaintiff prays for judgment as follows:

A. For an Order certifying this Action as a class action and appointing Plaintiff as class representative, and her counsel as class counsel;

B. For all available damages inclusive of disgorgement of profits, statutory damage and any other damages this Court may deem just and proper;

C. For injunctive relief ending the unlawful conduct as plead herein;

D. For attorneys' fees, costs, and other damages to be awarded in an amount to be determined as allowable by law;

E. Pre- and post-judgment interest on any amounts awarded; and,

F. Such other and further relief as this Court may deem just and proper.

VIII. JURY TRIAL DEMAND

53. Plaintiff Berger hereby demands a trial by jury.

DATED: December 2, 2022

Respectfully submitted,

/s/ Blake Hunter Yagman

Israel David
israel.david@davidllc.com
Blake Hunter Yagman
blake.yagman@davidllc.com
ISRAEL DAVID LLC

17 State Street, Suite 4010
New York, New York 10004
Tel.: (212) 739-0622
Facsimile: (212) 739-0628