

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

KAYLA MOLLER, individually, and on
behalf of all others similarly situated,

Plaintiff,

v.

COFFEE MEETS BAGEL, INC.,

Defendant.

Case No:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Kayla Moller (“Plaintiff”), individually and on behalf of all other person similarly situation, by her undersigned counsel, as and for her Class Action Complaint for violations of the Illinois Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/1 *et seq.*, against Defendant Coffee Meets Bagel, Inc. (“CMB” or “Defendant”), alleges on personal knowledge, due to investigation of her counsel, and, where indicated, on information and belief as follows:

NATURE OF THE ACTION

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in collecting, storing, and/or using her and others similarly situated individuals’ biometric identifiers¹ and biometric information² (referred to collectively at times as “biometrics”) without obtaining informed written consent or providing the requisite data retention and destruction policies, in direct violation of BIPA.

¹ “Biometric identifier” is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA, and “face geometry”, among others.

² “Biometric information” is any information captured, converted, stored, or shared based on a person’s biometric identifier used to identify an individual.

2. The Illinois Legislature has found that “[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information.”³ “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.”⁴

3. Coffee Meets Bagel (“CMB”) is an internet-based dating and social networking service and application that was founded in San Francisco in 2012. CMB claims to deliver high-quality matches with long-term potential. CMB states it creates a safe environment where its users feel comfortable to be their authentic selves.

4. In order to use the CMB dating application (“the App” or “CMB App”), CMB requires all its users, including Plaintiff, to create an account by first logging in with your Facebook account or by providing your phone number.

5. Curating a community for its users, CMB asks important details such as, but not limited to, education, interests, and family plans to create a detailed profile for each consumer user. CMB also requires its users, including Plaintiff, to verify their identities by uploading a self-photograph, i.e., a “selfie.” Users, including Plaintiff, can upload up to five to eight photos. Once a profile has been made, the application presents users with their first batch of user matches and helps users start conversations between them once matched.

6. Crucially, CMB scans the “selfie” photographs that users like Plaintiff provided and uploaded, creates a biometric template of the user’s face, and compares the user’s facial biometrics to the photographs which the user is posting in their online profile to verify the identity of all CMB

³ 740 ILCS 14/15(c).

⁴ *Id.*

users. This solution purportedly proactively detects scammers and bans fraudulent users before they compromise the community.

7. CMB has internal processes and employees/agents in place to help spot, investigate, and ban fraudulent users.

8. As of January 2024, CMB provided and/or provides the users' data to a third-party, Persona, an identity verification company, who may collect, capture, use, and store scans of users' facial geometry extracted from photos users uploaded, or scans of facial geometry or related biometric information extracted from the photos during the verification process.⁵

9. Upon information and belief, CMB's identity verification process requires users' data to leave their device.

10. By utilizing Persona, CMB can "check government IDs and selfie liveness in real time to make sure users are the right age and cross reference multiple risk signals to help [CMB] figure out whether to approve or decline users."⁶

11. Throughout this process, CMB collects, stores, possesses, uses, and disseminates its users' biometric data to ultimately improve its online dating platform, among other purposes, without obtaining written releases, consent, or authorization from its users or Plaintiff.

12. Due to the concerns over the security of individuals' biometrics the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Defendant may not obtain and/or possess an individual's biometrics unless it informs that person in writing that biometric identifiers or information will be collected or stored.⁷

⁵ <https://coffeemeetsbagel.com/privacy>

⁶ <https://withpersona.com/customers/coffee-meets-bagel>.

⁷ See 740 ILCS 14/15(b).

13. BIPA further requires that entities collecting biometrics must inform those persons in writing of the specific purpose and length of term for which such biometric identifiers or biometric information are being collected, stored, and used.⁸

14. Moreover, entities collecting biometrics must publish publicly available written retention schedules and guidelines for permanently destroying biometrics collected.⁹

15. The entity must store, transmit, and protect an individual's biometric identifiers and biometric information using the same standard of care in the industry and in a manner at least as protective as the means used to protect other confidential and sensitive information.¹⁰

16. Further, the entity is expressly prohibited from selling, leasing, trading, or otherwise profiting from an individual's biometrics.¹¹

17. Considering the irreplaceable nature of a user's biometric data, such as the facial geometry of Plaintiff, it cannot be altered or substituted if stolen or compromised.

18. In direct violation of each of the foregoing provisions of section 15(a) and 15(b) of BIPA, Defendant unlawfully collected, stored, and used – without first providing notice, obtaining informed written consent or publishing data retention policies – its user's biometric data, thus exposing them to significant and irreversible privacy risks.

19. In the event of a data breach or any other unauthorized access, if Defendant's database of its user's biometric data were compromised, the users to whom these sensitive and immutable biometric identifiers belong to could face identity theft, among other serious concerns.

⁸ *Id.*

⁹ *See* 740 ILCS 14/15(a).

¹⁰ *See* 740 ILCS 14/15(c).

¹¹ *See* 740 ILCS 15/15(c).

20. BIPA confers on Plaintiff and all other similarly situated Illinois residents a right to know of such risks, which are inherently presented by the collection, storage and dissemination of biometrics, and a right to know how long such risks will persist.

21. However, CMB never adequately informed Plaintiff or Class members of its biometrics collection practice of “face templates” (highly detailed geometric maps of a user’s face that is distinctive to a specific user, similarly to that of a fingerprint or voiceprint serves as an identifier for a person), never obtained the requisite written consent from Plaintiff or Class members regarding its biometric practices, and never provided any data retention or destruction policies to Plaintiff or Class members.

22. As broadly defined by BIPA, CMB is a “private entity” and is therefore obligated to adhere to all requirements of stipulated by BIPA.¹²

23. Plaintiff brings this action to prevent Defendant from further violating the privacy rights of Illinois residents and to recover statutory damages for Defendant’s unauthorized collection, storage, use, and dissemination of these individuals’ biometrics in violation of BIPA.

JURISDICTION AND VENUE

24. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the “Class Action Fairness Act”) because sufficient diversity of citizenship exists between the parties in this action, the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and there are 100 or more members of the Class. Because it is estimated that the Class will have at least hundred, if not thousands, of members and Defendant’s intentional and reckless violations of BIPA are punishable by statutory damages of \$5,000 per violation, the amount in controversy is well in excess of \$5,000,000.

¹² See 740 ILCS 14/10.

25. This Court has personal jurisdiction over Defendant because the wrongful conduct giving rise to this case occurred in, was directed to, and/or emanated from this District. Defendant collected data directly in Illinois from Plaintiff and exposed residents of Illinois to ongoing privacy risks within Illinois based on the collection, capture, obtainment, disclosure, redisclosure, and dissemination of the biometric identifiers and information.

26. Defendant's deliberate gathering of Illinois users' personally identifiable information is intentionally toward Illinois residents, including Plaintiff and the Class, and constitutes purposeful activity directed at devices and individuals in Illinois.

27. Venue is proper in this judicial district, a substantial part of the acts or omissions giving rise to Defendant's violations of BIPA took place within the State of Illinois and this judicial district.

28. Venue is also proper in this judicial district because Plaintiff is a citizen of the State of Illinois and Plaintiff seeks to vindicate Plaintiff's rights (and the rights of putative class members) as provided by BIPA.

29. Further, venue is proper in this judicial district because this Court has personal jurisdiction over Defendant.

PARTIES

30. Plaintiff Kayla Moller is and has been at all relevant times, a resident and citizen of Cook County in Illinois.

31. Defendant Coffee Meets Bagel, Inc. is a Delaware corporation with its principal place of business in San Francisco, California. Defendant conducts business through this County, the State of Illinois, and throughout the United States.

FACTUAL BACKGROUND

32. The Illinois General Assembly enacted BIPA in 2008 to establish standards of conduct for private entities that collect or possess biometric information.

33. A private entity, such as CMB, 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.¹³

34. BIPA defines “biometric identifier” as:

a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.¹⁴

¹³ 740 ILCS 14/15(a).

¹⁴ 740 ILCS 14/10.

35. BIPA defines “biometric information” as: “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.”¹⁵ Biometric information “does not include information derived from items or procedures excluded under the definition of biometric identifiers.”¹⁶

36. Under BIPA, 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:

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.¹⁷

37. 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.

38. Further, the Section 15(c) provides:

No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person’s or a customer’s biometric identifier or biometric information.¹⁸

39. BIPA also states:

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ See 740 ILCS 14/15(b).

¹⁸ 740 ILCS 14/15(c).

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.¹⁹

40. As alleged below, Defendant's practices of collecting, storing, and using individuals' biometric identifiers (specifically, facial geometry) and associated biometric information without informed written consent violated all three prongs of section 15(b) of BIPA. Defendant's failure to provide a publicly available written policy regarding their schedule and guidelines for the retention and permanent destruction of individuals' biometric identifiers and biometric information also violated section 15(a) of BIPA.

41. Unknown to CMB users, and in direct violation of section 15(b)(1) of BIPA, Defendant scanned and collected, and then indefinitely stored in an electronic database, a biometric template of Plaintiff's face and biometric identifiers when Plaintiff created her account.

42. Plaintiff joined CMB in 2018. When Plaintiff signed up and created her account profile, Plaintiff was required to upload a self-photograph, i.e., a "selfie." Plaintiff did so.

43. CMB then scanned Plaintiff's selfie, creating a biometric template of Plaintiff's face and other biometric identifiers, and compared the biometric identifiers to the selfie Plaintiff posted on her profile in order to verify Plaintiff's identity.

¹⁹ 740 ILCS 14/15(d).

44. On January 9, 2024, CMB updated their Privacy Policy to address photo verification and Biometrics, as well as but not limited to, CMB's use of the information, sharing of information, and data retention. CMB's Privacy Policy now states that CMB "provide[s] your data to a third-party, Persona, an identity verification company, who may use your information in accordance with its privacy policy, which you can review at <https://withpersona.com/legal/privacy-policy>. During this process, Persona may collect, capture, use, and store scans of your facial geometry extracted from photos you upload during the verification process, and retain any photos of identity documents you upload, photos of your face that you upload, or scans of facial geometry or related biometric information extracted from the photos during the verification process. We require Persona to destroy such data when these purposes have been satisfied, within no more than 3 years of your last interaction with Persona, unless otherwise required by law or legal process to retain the data."²⁰

45. However, CMB's previous Privacy Policy from June 11, 2021 did not have a policy regarding photo verification or biometrics, nor did it include a specific data retention policy regarding who had user's biometric identifiers or biometric information or the length of time for which their biometric identifiers or information would be collected, stored, and used. Nor did the privacy policy from June 2021 include its retention schedules or guidelines for permanently destroying any of these biometric identifiers and/or biometric information.²¹

46. In direct violation of sections 15(b)(2) and 15(b)(3) of BIPA, from at least approximately 2018 to at least approximately 2021, Defendant never informed Illinois resident who had their face geometry collected of the specific purpose and length of time for which their

²⁰ <https://coffeemeetsbagel.com/privacy>.

²¹ <https://web.archive.org/web/20230902011358/https://coffeemeetsbagel.com/privacy-terms/>

biometric identifiers or information would be collected, stored, and used, nor did Defendant obtain a written release from Plaintiff.

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

48. CMB has divulged, redistributed, or otherwise shared Plaintiff's biometric information under the following circumstances: 1) without Plaintiff's consent; 2) without Plaintiff's authorization for a financial transaction initiated or approved by Plaintiff; 3) without legal obligation by State or federal law or local statute; or 4) without being required pursuant to a valid warrant or subpoena issued by a court with jurisdiction.

49. Further, there is a significant risk that CMB has divulged, redistributed, or shared Plaintiff's biometric identifiers and/or biometric information to numerous third-party service providers for various business purposes, including but not limited to, those offering business or professional services, and technical support functions to CMB, without Plaintiff's knowledge or consent.

50. The collection and preservation of biometric information by CMB, as alleged herein, is not specific to Plaintiff but rather represents part of CMB's policies and protocols applied uniformly to all its users, including the Class members.

CLASS ALLEGATIONS

51. **Class Definition:** Plaintiff brings this action pursuant to 735 ILCS 5/2-801 on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

All individuals who had their biometric identifiers, iris, retina, facial geometry, or biometric information collected, captured, received, or otherwise obtained, stored and/or disclosed by Coffee Meets Bagel, Inc. while residing in Illinois.

52. **Numerosity:** Pursuant to 735 ILCS 5/2-801 (1), the number of persons within the Class is substantial, believed to amount to hundred or thousands of persons. It is therefore, impractical to join each member of the Class as a named Plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. The precise number of Class members is unknown at this time, but can be readily determined from Defendant's business records.

53. **Commonality and Predominance:** Pursuant to 735 ILCS 5/2-801(2), there are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any class member, include, but are not limited to, the following:

1. Whether Defendant collected or otherwise obtained Plaintiff's and the Class members' biometric identifiers and/or biometric information;
2. Whether Defendant properly informed Plaintiff and the Class members' that it collected, used, and stored their biometric identifiers and/or biometric information;
3. Whether Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, used, and store Plaintiff's and the Class members' biometric identifiers and/or biometric information;
4. Whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of their last interaction, which occurs first;
5. Whether Defendant used Plaintiff's and the Class members' biometric identifiers and/or biometric information to identify them;
6. Whether Defendant destroyed Plaintiff's and the Class members' biometric identifiers and/or biometric information once that information was no longer needed for the purpose for which it was originally collected; and
7. Whether Defendant's violation of BIPA were committed intentionally, recklessly, or negligently.

54. **Adequate Representation:** Pursuant to 735 ILCS 5/2-801 (3), Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex class action litigation. Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Class members and have the resources to do so. Neither Plaintiff nor their counsel have any interests adverse to those of the Class.

55. **Appropriateness:** Pursuant to 735 ILCS 5/2-801 (4), a class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class are likely to have been small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

CAUSES OF ACTION

COUNT ONE

Violation of the Illinois Biometric Information Privacy Act 740 ILCS 14/15(a) (On Behalf of Plaintiff and the Class)

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

57. Section 15(a) of the BIPA requires that any “private entity in possession of biometric identifiers . . . must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers . . . when the initial purpose for collecting or obtaining such identifiers . . . 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).

58. CMB does not publicly provide a retention schedule or guidelines for permanently destroying their biometric identifiers or biometric information as specified by the BIPA. *See* 740 ILCS 14/15(a).

COUNT TWO

Violation of the Illinois Biometric Information Privacy Act 740 ILCS 14/15(b) (On Behalf of Plaintiff and the Class)

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

60. The BIPA makes it unlawful for any private entity to, among other things, “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier . . . unless it first: (1) informs the subject . . . in writing that a biometric identifier . . . is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier . . . is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier” 740 ILCS 14/15(b).

61. CMB is a Delaware corporation and thus qualifies as a “private entity” under the BIPA. *See* 740 ILCS 14/10.

62. Plaintiff and the Class members’ facial geometry are “biometric identifiers” or “biometric information” pursuant to 740 ILCS 14/10.

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

64. CMB did not properly inform Plaintiff or the Class members in writing that their biometric identifiers or biometric information were being collected and stored, nor did it inform them in writing of the specific purpose and length of term for which their biometric identifiers or biometric information were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

65. By collecting, storing, and using Plaintiff's and the Class members' biometric identifiers or biometric information as described herein, CMB violated Plaintiff and the Class members' right to privacy in their biometric identifiers as set forth in the BIPA.

COUNT THREE
Violation of the Illinois Biometric Information Privacy Act 740 ILCS 14/15(d)
(On Behalf of Plaintiff and the Class)

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

67. The BIPA makes it unlawful for any private entity in possession of biometric identifiers or biometric information to "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).

68. Discovery will uncover the full extent of how Defendant disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class Members' biometric information. This includes disclosure to various third-party service providers for Defendants business purposes including third-party providers that provide business services, professional services, and technical support functions to Defendants.

69. Defendants' 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, Plaintiff Kayla Moller, on behalf of herself individually 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 her counsel as Class Counsel;
- B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*;
- C. Awarding statutory damages of \$5,000.00 for each and every intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if the Court finds that Defendant's violations were negligent;
- D. Awarding injunctive and other equitable relief as a necessary to protect the interests of the Class, including, *inter alia*, an Order requiring Defendant to collect, store, and use biometric identifiers and/or biometric information in compliance with BIPA; Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);

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

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

JURY DEMAND

Plaintiff and the Class members' hereby demands a trial by jury on all issues so triable.

Dated: April 15, 2024

By: */s/ Robert M. Foote, Esq.*
ROBERT M. FOOTE (#3124325)
BRET PUFAHL (#6325814)
KATHLEEN C. CHAVEZ (#6255735)
ELIZABETH C. CHAVEZ (#6323726)
**FOOTE, MIELKE, CHAVEZ
& O'NEIL, LLC**
1541 E. Fabyan Parkway, Suite 101
Geneva, IL 60134
Telephone: (630) 228-9091
Facsimile: (630) 232-7452
rmf@fmcolaw.com
bkp@fmcolaw.com
kcc@fmcolaw.com
ecc@fmcolaw.com

WILLIAM AUDET (CA SBN 117456)
LING Y. KUANG (CA SBN 296873)
AUDET & PARTNERS, LLP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 568-2555
Facsimile: (415) 568-1776
waudet@audetlaw.com
lkuang@audetlaw.com

Counsel for Plaintiff and the Proposed Class