

1 Leah M. Beligan (SBN 250834)
2 lbeligan@beliganlawgroup.com
3 Jerusalem F. Beligan (SBN 211258)
4 jbeligan@beliganlawgroup.com
5 **BELIGAN LAW GROUP, LLP**
6 19800 MacArthur Blvd., Ste. 300
7 Newport Beach, CA 92612
8 Telephone: (949) 224-3881

9 James L. Simon (*pro hac vice* forthcoming)
10 james@simonsayspay.com
11 **SIMON LAW CO.**
12 11 ½ N. Franklin Steet
13 Chagrin Falls, Ohio 44022
14 Telephone: (216) 816-8696

15 Michael L. Fradin (*pro hac vice* forthcoming)
16 mike@fradinlaw.com
17 **FRADIN LAW**
18 8401 Crawford Ave., Ste. 104
19 Skokie, IL 60076
20 Telephone: (847) 986-5889

21 *Attorneys for Plaintiff and the Putative Class*

22 **UNITED STATES DISTRICT COURT**
23 **NORTHERN DISTRICT OF CALIFORNIA**
24 **SAN JOSE DIVISION**

25 Ryan Murphy, individually, and on behalf of all) Case No. _____
26 others similarly situated,)
27)
28 Plaintiff,) **CLASS ACTION**
vs.) **COMPLAINT**
Jumio, Inc.,) **DEMAND FOR JURY TRIAL**
Defendant.)
_____)
_____)

29 **CLASS ACTION COMPLAINT**

30 Now comes Plaintiff Ryan Murphy ("Plaintiff"), on behalf of himself and all other similarly
31 situated, through Counsel, and pursuant to 735 ILCS §§ 5/2-801 and 2-802 and Fed. R. Civ. P. 23,
32 against Defendant Jumio, Inc. ("Jumio" or "Defendant"), its subsidiaries and affiliates, to redress
33 and curtail Defendant's unlawful collections, obtainments, use, storage, and disclosure of Plaintiff's
34 sensitive and proprietary biometric identifiers and/or biometric information (collectively referred to
35 herein as "biometric data" and/or "biometrics"). Plaintiff alleges as follows upon personal

1 knowledge as to himself, his own acts and experiences and, as to all other matters, upon information
2 and belief including investigation conducted by his attorneys.

3 **NATURE OF THE ACTION**

4 1. Defendant Jumio, Inc. is a Delaware corporation which operates as an information
5 “processor” for Coinbase. As a processor, Jumio is an entity that processes personal information on
6 behalf of Coinbase, based upon Coinbase’s instructions.

7 2. Plaintiff opened a Coinbase account within the five years immediately preceding
8 the filing of this matter and had his biometric information processed by Jumio as part of the
9 process of signing up for his account.

10 3. As part of signing up, and/or gaining access to his Coinbase account, Plaintiff was
11 required to upload a picture of (1) a valid state-issued identification; and (2) a real time portrait of
12 his face, i.e. a “selfie.”

13 4. Coinbase utilizes the services of Jumio, who then scans the “selfie” photograph,
14 creates a biometric template of the user’s face, and compares the user’s facial biometrics to the
15 photograph on the identification document to confirm whether they match.

16 5. Coinbase users, including Plaintiff, are instructed to setup biometric authentication
17 for use with Coinbase’s mobile app.

18 6. Jumio, acting as a processor for Coinbase, collects, stores, possesses, otherwise
19 obtains, uses, and disseminates its users' biometric data to, amongst other things, further enhance
20 Coinbase and its online “app-based” platform.

21 7. Facial geometry scans are unique, permanent biometric identifiers associated with
22 each user that cannot be changed or replaced if stolen or compromised. Jumio’s unlawful collection,
23 obtainment, storage, and use of its users' biometric data exposes them to serious and irreversible
24 privacy risks. For example, if Jumio’s database containing facial geometry scans or other sensitive,
25 proprietary biometric data is hacked, breached, or otherwise exposed, Jumio users have no means
26 by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this
27 highly personal and private information.

1 8. The Illinois legislature enacted BIPA to protect residents' privacy interests in their
2 biometric data. *See Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 963 (N.D. Ill. 2020),
3 citing *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, 432 Ill. Dec. 654, 129 N.E.3d 1197,
4 1199 (2019).

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

10 10. In recognition of these concerns over the security of individuals' biometrics –
11 particularly in the City of Chicago, which has been selected by major national corporations as a
12 “pilot testing site[] for new applications of biometric-facilitated financial transactions, including
13 finger-scan technologies at grocery stores, gas stations, and school cafeterias” (740 ILCS 14/5(b))
14 – the Illinois Legislature enacted the BIPA, which provides, *inter alia*, that a private entity like
15 Jumio may not obtain and/or possess an individual's biometrics unless it: (1) informs that person in
16 writing that biometric identifiers or information will be collected or stored; (2) informs that person
17 in writing of the specific purpose and length of term for which such biometric identifiers or biometric
18 information is being collected, stored and used; (3) receives a written release from the person for
19 the collection of his or her biometric identifiers or information; and (4) publishes publicly-available
20 written retention schedules and guidelines for permanently destroying biometric identifiers and
21 biometric information. 740 ILCS 14/15(a)-(b).

22 11. The Illinois Legislature has found that “[b]iometrics are unlike other unique
23 identifiers that are used to access finances or other sensitive information.” 740 ILCS 14/5(c). “For
24 example, social security numbers, when compromised, can be changed. Biometrics, however, are
25 biologically unique to the individual; therefore, once compromised, the individual has no recourse,
26 is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated
27 transactions.” *Id.*

1 Complaint occurred in the County of Santa Clara and Jumio is headquartered in the City of
2 Sunnyvale, California.

3 **FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS**

4 21. Plaintiff realleges and incorporates by reference all allegations in all preceding
5 paragraphs.

6 22. Plaintiff opened a Coinbase account within the five years immediately preceding the
7 filing of this action.

8 23. As part of signing up, and/or gaining access to his Coinbase account, Plaintiff was
9 required to upload a picture of (1) a valid state-issued identification; and (2) a real time portrait of
10 his face, i.e. a “selfie.”

11 24. Jumio, as a processor for Coinbase, then scanned Plaintiff’s “selfie” photograph,
12 creating a biometric template of the Plaintiff’s face and biometric identifiers, and compared
13 Plaintiff’s biometric identifiers to the photograph on his state issued identification document to
14 confirm whether they match.

15 25. Coinbase users, including Plaintiff, are instructed to setup biometric authentication
16 for use with Coinbase’s mobile app.

17 26. In other words, Jumio, as a processor for Coinbase, collected and retained biometric
18 information for the purpose of verifying Plaintiff’s identity prior to opening a Coinbase account in
19 Plaintiff’s name.

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

24 28. Ostensibly, the purpose of Jumio’s collection of Plaintiff’s facial geometry was to
25 verify Plaintiff’s identity prior to opening a Coinbase account in Plaintiff’s name.

26 29. As such, Plaintiff’s facial geometry should have been permanently destroyed by
27 Jumio following the opening of Plaintiff’s Coinbase account.

1 30. However, Jumio failed to permanently destroy Plaintiff’s facial geometry following
2 the opening of Plaintiff’s Coinbase account and instead retained Plaintiff’s biometric information.

3 31. As such, Jumio’s retention of Plaintiff’s biometric information was unlawful and in
4 violation of 740 ILCS § 14/15(a).

5 32. Coinbase did not inform Plaintiff in writing that Jumio was collecting or storing his
6 biometric information.

7 33. Instead, Coinbase simply instructed Plaintiff to upload his state issued identification
8 forms and “selfie” photographs as part of the overall account opening process.

9 34. In fact, Jumio made no mention of biometric information, collection of biometric
10 information, or storage of biometric information.

11 35. Moreover, Jumio did not inform Plaintiff in writing of the specific purpose and length
12 of term for which his biometric information was being collected, stored, and used.

13 36. Jumio collected, stored, and used Plaintiff’s biometric information without ever
14 receiving a written release executed by Plaintiff which would consent to or authorize Jumio to do
15 the same.

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

21 38. Upon information and belief, Jumio is part of numerous third parties, including
22 Onfido, Inc., Au10tix LTD, Solaris AG, and Liquid Co., Ltd., all of which have had Plaintiff’s
23 biometric information disclosed, redisclosed or otherwise disseminated to them via their role as a
24 processor for Coinbase.

25 39. Jumio’s collection and retention of biometric information as described herein is not
26 unique to Plaintiff and is instead part of Jumio’s policies and procedures which Jumio applies to all
27 of its users, including the Class Members.

RULE 23 CLASS DEFINITION AND ALLEGATIONS

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

41. Plaintiff brings Claims for Relief in violation of BIPA as a class action under Rule 23(a), (b)(2) and (b)(3). Plaintiff brings these claims on behalf of himself and all members of the following Rule 23 Class:

All Illinois residents who had their biometric information collected by Jumio while using the platform Coinbase at any point in the five (5) years preceding the filing of this Complaint.

42. 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.

43. **Numerosity (Rule 23(a)(1)).** 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.

44. **Existence of Common Questions of Law and Fact (Rule 23(a)(2)).** Common questions of law and fact exist as to Plaintiff and the Class Members including, but not limited to, the following:

- a. Whether Jumio 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 Jumio, whichever occurs first.
- b. Whether Jumio 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)

1 informing Plaintiff and the Class Members in writing of the specific purpose and
2 length of term for which their biometric identifiers or biometric information was
3 being collected, stored, and used; and (3) receiving a written release executed by
4 Plaintiff and the Class Members.

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

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

14 45. **Typicality (Rule 23(a)(3)).** Plaintiff's claims are typical of the Class Members'
15 claims. Plaintiff, like the Class Members, had his biometric identifiers and biometric information
16 collected, retained or otherwise possessed by Jumio without its adherence to the requirements of
17 BIPA as detailed herein.

18 46. **Adequacy (Rule 23(a)(4)).** Plaintiff will fairly and adequately represent and protect
19 the interests of the Class Members. Plaintiff has retained counsel competent and experienced in
20 complex class actions.

21 47. **Injunctive and Declaratory Relief (Rule 23(b)(2)).** Class certification of the Rule
22 23 claims is appropriate under Rule 23(b)(2) because Jumio acted or refused to act on grounds
23 generally applicable to the Class Members, making appropriate declaratory relief with respect to the
24 Class Members as a whole.

25 48. **Predominance and Superiority of Class Action (Rule 23(b)(3)).** Class
26 certification of the Rule 23 claims is also appropriate under Rule 23(b)(3) because questions of law
27 and fact common to the Class Members predominate over questions affecting only individual
28

1 members of the classes, and because a class action is superior to other available methods for the fair
2 and efficient adjudication of this litigation. Jumio's common and uniform policies and practices
3 illegally deprived Plaintiff and the Class Members of the privacy protections which BIPA seeks to
4 ensure; thus, making the question of liability and damages much more manageable and efficient to
5 resolve in a class action, compared to hundreds of individual trials. The damages suffered by
6 individual Class Members are small compared to the expense and burden of individual prosecution.
7 In addition, class certification is superior because it will obviate the need for unduly duplicative
8 litigation that might result in inconsistent judgments about Jumio's practices.

9 49. Plaintiff intends to send notice to all Class Members to the extent required by Fed.
10 R. Civ. P. 23.

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

12 50. Plaintiff realleges and incorporates by reference all allegations in all preceding
13 paragraphs.

14 51. A private entity in possession of biometric identifiers or biometric information must
15 develop a written policy, made available to the public, establishing a retention schedule and
16 guidelines for permanently destroying biometric identifiers and biometric information when the
17 initial purpose for collecting or obtaining such identifiers or information has been satisfied or within
18 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a
19 valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession
20 of biometric identifiers or biometric information must comply with its established retention schedule
21 and destruction guidelines. 740 ILCS § 14/15(a).

22 52. Jumio created and collected biometric templates of the Plaintiff's and the Class
23 Members' faces which qualifies as biometric information as defined by BIPA.

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

1 54. Ostensibly, the purpose of Jumio’s collection of Plaintiff’s and the Class Members’
2 facial geometry was to verify Plaintiff’s and the Class Members’ identities prior to opening a
3 Coinbase account in their names.

4 55. As such, Plaintiff’s and the Class Members’ facial geometry should have been
5 permanently destroyed by Jumio following the opening of their Coinbase accounts.

6 56. However, Jumio failed to permanently destroy Plaintiff’s and the Class Members’
7 facial geometries following the opening of their Jumio accounts and instead retained Plaintiff’s and
8 the Class Members’ biometric information.

9 57. Moreover, Plaintiff’s and the Class Members’ biometric information should have
10 been permanently destroyed by Jumio after Plaintiff and the Class Members logged out or ceased
11 using Coinbase.

12 58. However, Jumio failed to permanently destroy Plaintiff’s and the Class Members’
13 fingerprints after they logged out or ceased using the Coinbase mobile app.

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

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

17 70. Plaintiff realleges and incorporates by reference all allegations in all preceding
18 paragraphs.

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

- 21 (1) informs the subject or the subject's legally authorized representative in writing
22 that a biometric identifier or biometric information is being collected or stored;
- 23 (2) informs the subject or the subject's legally authorized representative in writing
24 of the specific purpose and length of term for which a biometric identifier or
25 biometric information is being collected, stored, and used; and
- 26 (3) receives a written release executed by the subject of the biometric identifier or
27 biometric information or the subject's legally authorized representative. 740 ILCS §
28 14/15(b).

1 72. Jumio did not inform Plaintiff and the Class Members in writing that Jumio was
2 collecting or storing their biometric information.

3 73. Instead, Jumio simply instructed Plaintiff and the Class Members to upload their state
4 issued identification forms and “selfies” as part of the overall account opening process and this
5 information was then processed by Jumio by creating biometric facial templates.

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

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

12 76. As such, Jumio’s collection of Plaintiff’s and the Class Members’ biometric
13 information was unlawful and in violation of 740 ILCS § 14/15(b).

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

15 77. Plaintiff realleges and incorporates by reference all allegations in all preceding
16 paragraphs.

17 78. No private entity in possession of a biometric identifier or biometric information may
18 disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or
19 biometric information unless:

20 (1) the subject of the biometric identifier or biometric information or the subject's
21 legally authorized representative consents to the disclosure or redisclosure;

22 (2) the disclosure or redisclosure completes a financial transaction requested or
23 authorized by the subject of the biometric identifier or the biometric information or
the subject's legally authorized representative;

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

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

1 79. While discovery will ascertain all of the ways in which Jumio disclosed, redisclosed,
2 or otherwise disseminated Plaintiff’s and the Class Members’ biometric information, Jumio
3 disclosed, redisclosed, or otherwise disseminated Plaintiff’s and the Class Members’ biometric
4 information to numerous third parties including, but not limited to, Onfido, Inc., Au10tix LTD,
5 Solaris AG, and Liquid Co., Ltd.

6 80. Jumio’s disclosures, redisclosures, or otherwise disseminating of Plaintiff’s and the
7 Class Members’ biometric information was unlawful and in violation of 740 ILCS § 14/15(d).

8 **WHEREFORE**, individually, and on behalf of the Class Members, Plaintiff prays for: (1)
9 certification of this case as a class action pursuant to Fed. R. Civ. P. 23 and appointing the
10 undersigned counsel as class counsel; (2) a declaration that Defendant has violated BIPA, 740 ILCS
11 14/1 *et seq.*; (3) statutory damages of \$5,000.00 for the intentional and reckless violation of BIPA
12 pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of \$1,000.00 per violation,
13 pursuant to 740 ILCS 14/20(1) in the event the court finds that Defendant’s violations of BIPA were
14 not willful; (4) reasonable attorneys’ fees and costs and other litigation expense pursuant to 740
15 ILCS 14/20(3); (5) actual damages; and (6) for any other relief deemed appropriate in the premises.

16 **DEMAND FOR JURY TRIAL**

17 Plaintiff and the Class Members hereby demand a jury trial on all causes of action and claims
18 with respect to which they each have a state and/or federal constitutional right to a jury trial.

19 Dated: February 9, 2024

BELIGAN LAW GROUP, LLP

21 By: /s/ Leah M. Beligan
Leah M. Beligan (SBN 250834)
22 lbeligan@beliganlawgroup.com
Jerusalem F. Beligan (SBN 211258)
23 jbeligan@beliganlawgroup.com
19800 MacArthur Blvd., Ste. 300
Newport Beach, CA 92612
24 Telephone: (949) 224-3881

25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FRADIN LAW

By: /s/ Michael L. Fradin
Michael L. Fradin (*pro hac vice*
forthcoming)
8 N. Court St., Suite 403
Athens, Ohio 45701
Telephone: 847-986-5889
Email: mike@fradinlaw.com

SIMON LAW CO.

By: /s/ James L. Simon
James L. Simon (*pro hac vice*
forthcoming)
11 1/2 N. Franklin Street
Chagrin Falls, Ohio 44022
Telephone: (216) 816-8696
Email: james@simonsayspay.com

Attorneys for Plaintiff and the Putative Class

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Coinbase Info Processor Jumio Fails to Destroy Facial Scans Once Account Identities Are Verified, Class Action Claims](#)
