

**NO
EXHIBITS**

CASE NO. 218CH07116

DATE: 6/5/2018

CASE TYPE: Class Action

PAGE COUNT: 17

CASE NOTE

**IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION**

JACK GLYNN, individually and on behalf of a)
class of similarly situated individuals,)
))
Plaintiff,))
))
v.))
))
eDRIVING, LLC, a Delaware limited liability)
corporation,)
))
Defendant.)

No. 2018CH07116
CALENDAR/ROOM 04
TIME 00:00
Hon. Class Action

CLASS ACTION COMPLAINT & JURY DEMAND

Plaintiff Jack Glynn, both individually and on behalf of other similarly situated individuals, brings this Class Action Complaint against Defendant eDriving, LLC d/b/a Driversed.com (“Defendant”), to stop Defendant’s capture, collection, use, and storage of individuals’ biometric identifiers and/or biometric information in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (the “BIPA”), and to obtain redress for all persons injured by its conduct. Plaintiff alleges as follows based upon personal knowledge as to his own act and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

FILED
JUN 29 AM 4:08
DOFOTHY BROWN CLERK

INTRODUCTION

1. This case is about an online driver’s education provider capturing, collecting, storing, and using Plaintiff’s and other students’ biometric identifiers and/or biometric information without regard to BIPA and the concrete privacy rights and pecuniary interests that BIPA protects. Defendant collects its students’ unique voiceprints immediately upon registration without complying with BIPA’s requirements.

2. Following the 2007 bankruptcy of a company specializing in the collection and use of biometric information, which risked the sale or transfer of millions of fingerprint records to the highest bidder, the Illinois Legislature passed BIPA, a statute of reasonable regulations addressing the collection, use and retention of biometric identifiers, such as voiceprints, by private entities, such as Defendant.

3. The Illinois Legislature passed BIPA to provide consumers with statutory protection of their privacy rights; to ensure that they would receive certain disclosures before a private entity could collect, obtain and/or use their biometrics; to decrease the risk of a misappropriation of one's identity or a similar compromise of one's privacy; and to ensure that individuals whose biometrics were being collected, obtained and/or used could provide informed consent and be fully aware of how their biometrics were being handled and disposed of.

4. Indeed, the Illinois Legislature passed BIPA in part because "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5. For example, even sensitive information like Social Security numbers, when compromised, can be changed. "Biometrics, however, are biologically unique to each individual; therefore, once compromised, the individual has no recourse, is at a heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions. *Id.*

5. A "biometric identifier" is any personal feature that is unique to an individual and includes fingerprints, iris scans, palm scans, and DNA, among others. "Biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier which is used to identify an individual. 740 ILCS § 14/10.

6. As biometric technology has continued to develop over the past decade, biometrics are becoming more mainstream and are no longer relegated to esoteric corners of commerce. Many

businesses and financial institutions have incorporated biometric applications into their consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

7. In recognition of the concern over the security of individuals' biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that private entities, such as Defendant, may not obtain and/or possess an individual's biometrics unless they first:

(1) informs that person in writing that biometric identifiers or biometric information will be collected or stored;

(2) informs that person in writing of the specific purpose and the length of term for which such biometric identifiers for biometric information is being collected, stored and used;

(3) receives a written release from the person for the collection of their biometric identifiers or biometric information; and

(4) if a private entity, such as Defendant, publishes a publicly available retention schedule and guidelines for permanently destroying biometric identifiers and biometric information.

740 ILCS 14/5.

8. In direct violation of the foregoing provisions, Defendant actively captures, collects, stores, and uses, without obtaining informed written consent, the biometrics of hundreds of Illinois residents whose voiceprints are captured and stored for identity-verification purposes, and continues to require use of said voiceprint throughout the duration of the course.




9. Defendant is an online driver's education provider. As shown below, in order to verify that a given student is the individual actually taking Defendant's online course (as opposed to some third person), Defendant asks students to provide a voice sample by telephone immediately upon registration.

 **Create Your Voice Password**

The state of Illinois requires us to verify the identity of the person taking this course. You will now call us to create a voice password.

Please read this carefully before you call:

- Make sure you're in a quiet place without background noise.
- When you call the toll-free number, you will be asked to enter the PIN shown below.
- Follow the operator's instructions to record your voice password. You will need to create a few samples, so don't worry if you are asked to repeat yourself.
- Speak in your normal voice. This is your personal voice password.

-  **Call**
1-888-672-6953
-  **Enter this PIN when asked:**
431749
-  **Follow instructions to record your voice password**

If you have any problems with our verification system,
please contact our customer service team for assistance at 1-888-651-2886.

10. Defendant uses students' voice samples to create voiceprints of each registered student and requires students to verify their identity by phone at several points throughout the course.

11. Defendant chooses to use voiceprints to verify students' identities instead of other common, less-intrusive verification methods such as requiring students to answer personal security questions.

12. The individual voiceprints are unique to each of Defendant's students, and Defendant's capture, collection, storage, and use of those biometric identifiers violates each student's substantive privacy rights protected under BIPA and exposes those individuals to serious and irreversible privacy risks—risks that BIPA was designed to avoid — including the ever-present risk of a data breach of Defendant's systems which would expose students' biometrics to hackers and other wrongdoers worldwide.

13. Defendant's practice of collecting voiceprints from its students is unlawful and a serious invasion of its students' right to privacy concerning their biometric information. Defendant failed to provide the disclosures required under BIPA by (1) failing to disclose to its students that

it was collecting their biometric identifiers, (2) failing to disclose to its students how long it intended to keep this highly sensitive information, (3) failing to obtain a written release from its students for its collection of the same.

14. Unlike a Social Security number, which can be changed, no amount of time or money can compensate Plaintiff, and other similarly situated individuals, if their voiceprints are compromised by the lax procedures through which Defendant captures, collects, stores, and uses its students' biometrics.

15. Had Plaintiff known that Defendant would capture, collect, store, and use his sensitive biometrics, he either would not have subscribed for Defendant's course or would not have paid Defendant the amount he did in order to register for Defendant's course.

16. On behalf of himself and the proposed class defined below, Plaintiff seeks an injunction requiring Defendant to destroy the Class members' biometrics in Defendant's possession, to cease all unlawful activity related to the capture, collection, storage, and use of his and other Class members' biometrics in Defendant's possession, to cease all unlawful activity related to the capture, collection, storage, and use of his and other Class members' biometrics and an award of statutory damages to the Class members, together with costs and reasonable attorneys' fees.

PARTIES

17. At all relevant times, Defendant eDriving, LLC is a Delaware limited liability corporation transacting business in Cook County, Illinois and has transacted business with prospective Illinois driver's education students using a site known as DriversEd.com.

18. At all relevant times, Plaintiff Jack Glynn has been a resident and citizen of the State of Illinois.

JURISDICTION AND VENUE

19. This court may assert personal jurisdiction over Defendant pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendant is conducting educational programs specifically marketed to prospective Illinois drivers, and because Plaintiff's claims arise out of such advertisement, as Defendant solicited Plaintiff's and Class Member's biometric information solely in relation to its Illinois Adult Drivers Course. Further, Defendant collected Plaintiff's and Class Member's biometric information as a result of telephone calls made in Illinois.

20. Venue is proper in Cook County because Plaintiff resides in Cook County and a substantial part of the events giving rise to Plaintiff's claims occurred in this District, as Defendant collected Plaintiff's biometric information during a telephone call Plaintiff made while present in Cook County.

BACKGROUND

21. Illinois enacted BIPA to regulate entities like Defendant that collect, store and use biometric identifiers and biometric information, including fingerprints, iris scans, and handprints.

22. Under BIPA, private entities may not collect, capture, purchase, receive through trade, or otherwise obtain a person's biometric identifier or biometric information unless they first:

(1) Inform the person in writing that a biometric identifier or biometric information is being collected;

(2) Inform the person in writing of the specific purpose and length of time for which a person's biometric identifier and/or biometric information is being captured, collected, stored, and used; and

(3) Receive a written release executed by the subject of the biometric identifier or biometric information providing consent.

740 ILCS 14/15(b).

23. Section 15(a) of BIPA also requires that a private entity in possession of biometric identifiers or biometric information develop:

- (1) A written policy;
- (2) Available to the public;
- (3) Which establishes a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information;
- (4) Within three years of the individual's last interaction with the private entity, or when the initial purpose of for collecting or obtaining biometric identifiers and/or biometric information has been satisfied.

740 ILCS 14/15(a).

24. Defendant is a "private entity" as that term is defined under BIPA. *See* 740 ILCS 14/10.

25. Whenever a student who registers for any of Defendant's Illinois Drivers Course, Defendant requires that the student call a specific phone number in order to provide a "voice password." Specifically, Defendant tells its registered students: "You will need to create a few samples, so don't worry if you are asked to repeat yourself."

26. Upon information and belief, Defendant uses its biometric identity verification system to capture the voiceprint of all students taking its course, including Plaintiff, uploading the information into Defendant's biometric devices, which captured, stored, and used said voiceprints.

27. Unlike other methods of verification such as personal security questions, etc. — which can be changed or replaced if stolen or compromised—voiceprints are unique, permanent biometric identifiers associated with the individual. Defendant's actions violate individuals' substantive privacy rights protected under BIPA and exposes Plaintiff and other individuals to serious and irreversible privacy risks.

28. The privacy risks associated with a person's biometrics are unparalleled — such information is more sensitive than a social security number, a passport, a birth certificate, etc. As such, Illinois' BIPA statute requires private entities to provide certain disclosures and obtain a written release from individuals prior to collecting their biometric identifiers and/or biometric information. Accordingly, BIPA protects individuals' right to be informed with respect to the capture, collection, storage, and use of their biometric identifiers, allowing them to make more informed decisions as to the circumstances under which they agree to provide their biometric identifiers and/or biometric information.

29. BIPA mandates that entities that engage in the use of biometric systems do so with reasonable safeguards after receiving informed consent to take such biometric information from the individual.

30. Defendant's practice of collecting, capturing, storing, and using its students' biometric identifiers and/or biometric information is unlawful under BIPA because such practices fail to satisfy each of the enumerated requirements described above, and therefore severely infringe on its students' right to privacy regarding their biometric identifiers and biometric information.

FACTS SPECIFIC TO PLAINTIFF

31. As Plaintiff had not yet acquired an Illinois driver's license, he was interested in gaining a certificate of completion of such a course that he could use as part of an application for an Illinois Driver's License.

32. Plaintiff visited Defendant's website, DriversEd.com and confirmed that Defendant offered an "Illinois Adult Driver's Education" for Illinois prospective drivers between the ages of 18 and 21 for which he paid \$63.00 to register.

33. Immediately after paying the course fee, Plaintiff was directed to the below page requiring him to call Defendant and provide a "voice password" or "voice sample."

Illinois Adult Drivers Course

[▶ Course Options](#)

Create Your Voice Password

The state of Illinois requires us to verify the identity of the person taking this course. You will now call us to create a voice password.

Please read this carefully before you call:

- Make sure you're in a quiet place without background noise.
- When you call the toll-free number, you will be asked to enter the PIN shown below.
- Follow the operator's instructions to record your voice password. You will need to create a few samples, so don't worry if you are asked to repeat yourself.
- Speak in your normal voice. This is your personal voice password.



Call

1-888-672-6953



Enter this PIN when asked:

431749



Follow instructions to record your voice password

If you have any problems with our verification system,
please contact our customer service team for assistance at 1-888-651-2886.

34. Defendant used Plaintiff's phone to call to create a unique voiceprint attributable to Plaintiff.

35. Prior to obtaining Plaintiff's biometric identifiers and/or information, Defendant did not inform him in writing that a biometric identifier or biometric information was being

captured, collected, stored, or used, nor did Defendant make its policies concerning biometric collection, retention and use of such sensitive information publicly available, as required by BIPA.

36. Prior to collecting Plaintiff's voiceprint, Defendant did not make a written policy available to the individuals or to the public establishing a retention schedule and guidelines for permanently destroying the biometric identifiers and biometric information that it collects, as required by BIPA. 740 ILCS 14/15(a).

37. Additionally, Defendant did not obtain consent for any transmission to third parties of Plaintiff's and other individuals' biometrics. To the extent Defendant utilized out of state vendors to operate its voiceprint verification program in conformance with biometric industry practice, Defendant has also violated BIPA on each occasion that it transmits such information to third parties.

38. Further, Defendant has required Plaintiff to make a telephone call and verify his identity by using his voice. Defendant used Plaintiff's previously provided voiceprint to verify his identity later in the course. Each subsequent use of Plaintiff's voiceprint, to verify his identity, qualifies as a violation of BIPA necessitating statutory damages.

39. To this day, Plaintiff is unaware of the status of his biometric information that was obtained by Defendant. Defendant has not informed him whether it still retains his biometric information, and if it does, for how long it intends to retain such information with his consent.

40. On information and belief, Defendant does not have a policy of informing individuals in any way what happens to their biometric information after it is collected and obtained, whether the information is transmitted to a third party and, if so, which third party, and what would happen to the data and information if an individual discontinues or finishes the driving

course, if Defendant's facilities were to close, or if Defendant was to be acquired, sold, or file for bankruptcy.

41. Plaintiff's biometric information is economically valuable and such value will increase as the commercialization of biometrics continues to grow. As such, Plaintiff did not receive the benefit of his bargain with Defendant because Plaintiff would not have provided Defendant with his biometrics had he been fully informed of BIPA and the taking of his biometric information, as required by the statute.

42. By knowingly and willfully failing to comply with the BIPA's mandatory notice, release, and policy publication requirements, Defendant has violated its students' substantive privacy rights protected under the BIPA, and as a result, Plaintiff and the other members of the Class have continuously been exposed to substantial and irreversible loss of privacy by Defendant's retention of their biometric information without their consent, with such constant and ongoing exposure constituting a severe harm and violation of their rights.

CLASS ALLEGATIONS

43. Plaintiff brings this action on behalf of himself and similarly situated individuals pursuant to 735 ILCS § 5/2-801. Plaintiff seeks to represent a Class defined as follows:

The Class: All individuals in Illinois whose biometrics were captured, collected, obtained, stored or used by Defendant within the applicable limitations period.

44. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officer or director.

45. Upon information and belief, there are hundreds, if not thousands, of members of the Class, making the members of the Class so numerous that joinder of all members is

impracticable. Although the exact number of members of the Class is currently unknown to Plaintiff, the members can be ascertained through Defendant's records.

46. Plaintiff's claims are typical of the claims of the Class members they seek to represent because the factual and legal bases of Defendant's liability to Plaintiff and the other Class members are the same and because Defendant's conduct has resulted in similar injuries to Plaintiff and to the Class. As alleged herein, Plaintiff and the other putative Class members have all suffered damages as a result of Defendant's BIPA violations.

47. There are many questions of law and fact common to the claims of Plaintiff and the other Class members, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not limited to, the following:

- a. Whether Defendant collects, captures, stores, or uses the biometrics of Class members;
- b. Whether Defendant developed and made available to the public a written policy which establishes a retention schedule and guidelines for permanently destroying biometric identifiers and information as required by BIPA;
- c. Whether Defendant obtained a written release from Class members before capturing, collecting, or otherwise obtaining individual's biometrics;
- d. Whether Defendant provided a written disclosure to individuals that explains the specific purposes, and the length of time, for which their biometrics were being collected, stored and used before taking their biometrics;
- e. Whether Defendant's conduct violates BIPA;
- f. Whether Defendant's violations of BIPA are willful and reckless; and

g. Whether Plaintiff and the Class members are entitled to damages and injunctive relief.

48. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

49. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class he seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

50. Defendant has acted and failed to act on grounds generally applicable to the Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I

Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*, (on behalf of Plaintiff and the Class)

51. Plaintiff incorporates by reference the foregoing allegations as if fully set forth herein.

52. BIPA requires private entities, such as Defendant, to obtain informed written consent from individuals before acquiring their biometric information. Specifically, BIPA makes

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

53. The BIPA also requires that private entities in possession of biometric identifiers and/or biometric information establish and maintain a publicly available retention policy. Entities which possess biometric identifiers or information must (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric information (entities may not retain biometric information longer than three years after the last interaction with the individual); and (ii) must adhere to the publicly posted retention and deletion schedule.

54. Defendant is a “private entity” as that term is defined under the BIPA. *See* 740 ILCS 14/10.

55. Plaintiff and the other Class members have had their “biometric identifiers,” namely their voiceprints, collected, captured, received or otherwise obtained by Defendant. Plaintiff’s and the other Class members’ biometric identifiers were also used to identify them, and therefore constitute “biometric information” as defined by the BIPA. 740 ILCS 14/10.

56. Additionally, beyond Defendant’s immediate post-registration collection of Plaintiff’s and Class members’ voiceprints, every instance that Defendant required Plaintiff and the other Class members to verify their identity by matching their voices with their respective

stored voiceprints, Defendant captured, collected, stored, and/or used Plaintiff's and the Class members' biometric identifiers or biometric information without valid consent and without complying with and, thus, in violation of the BIPA.

57. Defendant's practice with respect to capturing, collecting, storing, and using biometric identifiers and biometric information fails to comply with applicable BIPA requirements. Specifically, with respect to Plaintiff and the other Class members, Defendant failed to:

- a. Obtain the written release required by 740 ILCS 14/15(b)(3);
- b. Inform Plaintiff and the Class members in writing that their biometric identifiers and/or biometric information were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(1);
- c. Inform Plaintiff and the Class in writing of the specific purpose for which their biometric information and/or biometric identifiers were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);
- d. Inform Plaintiff and the Class in writing of the specific length of term their biometric information and/or biometric identifiers were being captured, collected, stored and used, as required by 740 ILCS 14/15(b)(2); and
- e. Provide a publicly available retention schedule detailing the length of time biometric information is stored and guidelines for permanently destroying the biometric information it stores, as required by 740 ILCS 14/15(a).

58. By capturing, collecting, storing, and using Plaintiff's and the other Class members' biometric identifiers and/or biometric information as described herein, Defendant violated

Plaintiff's and the other Class members' respective rights to privacy as set forth in the BIPA. 740 ILCS 14/15(a).

59. BIPA provides for statutory damages of \$5,000 for each willful and/or reckless violation of the BIPA and, alternatively, damages of \$1,000 for each negligent violation of the BIPA. 740 ILCS 14/20(1).

60. Defendant's violations of the BIPA, as set forth herein, were knowing and willful, or were in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with the BIPA disclosure, consent, and policy posting requirements.

PRAYER FOR RELIEF

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

- a. Certifying the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;
- b. Declaring that Defendant's actions, as set forth herein, violate the BIPA;
- c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with the BIPA requirements for the capture, collection, storage, and use of biometric identifiers and biometric information, including an injunction requiring Defendant to permanently destroy all biometric information of Plaintiff and of Class members in their possession and compensation in an amount to be determined at trial for the commercial value of Plaintiff's biometric information;
- d. Awarding statutory damages of \$5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(1);

- e. Awarding statutory damages of \$1,000 for each negligent violation of the BIPA, pursuant to 740 ILCS 14/20(3);
- f. Awarding reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);
- g. Awarding pre- and post-judgment interest, as allowable by law; and
- h. Awarding such further and other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Dated: June 5, 2018

Respectfully submitted,

JACK GLYNN, individually and on behalf of a
class of similarly situated individuals

By: 
One of Plaintiff's Attorneys

William P. Kingston
Jad Sheikali
MCGUIRE LAW, P.C.
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
Fax: (312) 275-7895
wkingston@mcgpc.com
jsheikali@mcgpc.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: [Online Driving School Hit with Class Action Over Alleged IL Biometric Privacy Violations](#)
