12-Person Jury

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

NICHOLAS HEGER, individually and on behalf of similarly situated individuals, *Plaintiff,* v. CHECKPOINTID, INC., a Delaware corporation, IDSCAN.NET, INC., a Delaware corporation, *Defendants.*	No. 2023CH02489 Hon. **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff Nicholas Heger ("Plaintiff"), both individually and on behalf of other similarly situated individuals, brings this Class Action Complaint against Defendants CheckpointID, Inc. and IDScan.net, Inc., (together "Defendants") for their violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(a)-(e) ("BIPA"). Plaintiff alleges the following based on personal knowledge as to Plaintiff's own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by their attorneys.

INTRODUCTION

A. BIPA.

1. Biometrics refer to unique personally identifying features such as a person's voiceprint, fingerprint, facial geometry, iris, among others.

2. The Illinois Legislature enacted BIPA because it found that "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, even sensitive information like Social Security numbers can be changed. Biometrics,

however, are biologically unique to each individual and, once compromised, such individual has no recourse, is at a heightened risk for identity theft, and is likely to withdraw from biometric facilitated transactions." 740 ILCS 14/5.

3. BIPA defines a "biometric identifier" as any personal feature that is unique to an individual, including voiceprints, fingerprints, facial scans, handprints, and palm scans. "Biometric information" is any information based on a biometric identifier, regardless of how it is converted or stored. 740 ILCS § 14/10. Collectively, biometric identifiers and biometric information are known as "biometrics."

4. To protect individuals' biometrics, BIPA provides, *inter alia*, that private entities, such as Defendant, may not obtain and/or possess an individual's biometrics unless they first: (1) inform the person whose biometrics are collected in writing that biometric identifiers or biometric information will be collected or stored; (2) inform them, in writing, of the specific purpose and the length of time for which such biometrics are being collected, stored and used; (3) receive a written release allowing them to capture and collect the biometrics; and (4) publish a publicly available retention policy for permanently destroying biometrics when their use 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).

5. BIPA's Compliance requirements are straightforward and easily satisfied, often requiring little more than acquiring a written record of consent to a company's BIPA practices.

B. Defendants' Biometric Collection Practices.

6. Defendant CheckpointID, Inc. ("Checkpoint") is a provider of identity verification services for property management companies.

7. Defendant IDScan.net, Inc. ("IDScan") is a provider of biometric authentication technology for entities such as Checkpoint.

8. Together, Defendants provided an automated biometric identity verification service that allowed property management companies to verify potential housing applicants' identities.

9. Defendants' identity verification service works by using an applicant's cell phone to take a picture of their face from which it extract the applicant's unique facial geometry, and then compares the extracted facial biometric template with the facial biometrics obtained from a driver's license or other identity document that features the applicant's face to confirm that they match.

10. However, while Defendants obtained the facial biometrics of Illinois residents such as Plaintiff as part of housing applications for Illinois rental residences, until recently Defendants failed to comply with BIPA's regulations and did not obtain individuals' consent to gather their facial biometrics.

11. Nor did Defendants maintain a publicly available data retention policy that disclosed what they did with the facial biometrics they obtained or how long they were stored for.

12. Plaintiff seeks on behalf of himself and the proposed Class defined below, an injunction requiring Defendants compliance with BIPA, as well as an award of statutory damages to the Class, together with costs and reasonable attorneys' fees.

PARTIES

13. Defendant CheckpointID, Inc. is a Delaware corporation that conducts business throughout Illinois, including in Cook County, Illinois.

14. Defendant IDScan.net, Inc. is a Delaware corporation that conducts business throughout Illinois, including in Cook County, Illinois.

15. At all relevant times, Plaintiff Nicholas Heger has been a resident and a citizen of the state of Illinois.

JURISDICTION AND VENUE

16. This Court may assert personal jurisdiction over Defendants pursuant to 735 ILCS 5/2-209 in accordance with the Illinois Constitution and the Constitution of the United States, because Defendants conduct business within this state and because Plaintiff's claims arise out of Defendants' unlawful in-state actions, as Defendants captured, collected, stored, and used Plaintiff's biometric identifiers and/or biometric information in this state.

17. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101, because Defendants conduct business in Cook County and thus reside there under § 2-102.

FACTUAL BACKGROUND

18. Defendants are a provider of a biometric identity verification service to property management companies across the United States, and throughout Illinois.

19. Specifically, Defendants' service allows property management companies to verify that applicants for housing are the same person who they disclose on their rental/housing applications.

20. Defendants' biometric identity verification system operates by first sending a text message to the property applicant's cell phone at its customer's request.

21. The property applicant receives a text message with a link that directs them to a website hosted by Checkpoint.

22. The website directs the user to use their phone's camera to take a picture of the front and of the back of their driver's license or other government issued identification that features a picture of their face.

23. After the applicant has uploaded pictures of their ID, the webpage interacts with the applicant's phone and automatically asks the applicant to allow it to access the phone's front facing camera.

24. Once the applicant allows the website access to their camera, their face immediately appears in an oval window on the website, and a virtual geometric pattern appears over the applicant's face indicating that the applicant's facial biometrics are being gathered. The applicant is then asked to turn their head to the left and to the right.

25. When the applicant's facial biometrics are sufficiently recorded, the applicant is informed that their verification process is complete.

26. On the back end, and undisclosed to the applicant, when the applicant uploads a picture of their ID document that features their face, Defendants' biometric verification system gathers a geometric template of the applicant's face from their ID document and compares it to the geometric template of the applicant's face that it gathers from their front facing camera to see if they match.

27. Critically, even though during the relevant time period Defendants obtained the facial biometrics of thousands of Illinois residents, including Plaintiff and the other Class members, Defendants entirely failed to obtain written consent to do so as required by BIPA.

28. Indeed, at no point during the verification process did Defendants present any sort of prompt asking the applicant for consent to gather their facial biometrics.

29. Nor did Defendants make publicly available a policy as to Defendants' collection, storage, deletion, retention, and security practices regarding the facial biometric information in their possession.

30. Defendants also unlawfully profited from the facial biometrics they obtained, including Plaintiff's and the other Class' members, as Defendants were paid to verify the applicants' facial biometrics.

31. Checkpoint appears to have only recently instituted a publicly available data policy regarding the biometrics that it gathers from its customers' property applicants sometime after December 2022. *See* https://web.archive.org/web/20221203212635/https://mrisoftware.checkpointid.com/ (showing that Checkpoint's website did not feature a "facial scan policy") versus https://mrisoftware.checkpointid.com/ (Checkpoint's current website featuring a "facial scan policy" at the bottom of the page and available at https://info.mrisoftware.com/facial-scan-policy).

32. IDScan, however, appears to still have no publicly available biometric policy. *See* https://idscan.net/privacy-policy/.

FACTS SPECIFIC TO PLAINTIFF

33. In or about May 2022 Plaintiff Heger applied to rent an apartment in Cobbler Square Lofts in Chicago, Illinois.

34. As part of the application process, and while he was located in and residing in Illinois, Plaintiff received a link on his cell phones directing him to Checkpoint's website to verify his identity.

35. Like thousands of other Illinois residents who had to verify their identity through Defendants' automated biometric identity verification system, Plaintiff used his cell phone to provide a picture of the front and back of his driver's license to the system through the website.

36. Plaintiff then had to give Defendants' verification system access to the front facing camera of his phone, at which point it obtained a geometric template of Plaintiff's face.

37. After Plaintiff's facial biometrics were gathered by Defendants and verified as matching his driver's license, he was informed that the verification process was complete.

38. Plaintiff, like the thousands of other Illinois property applicants who are members of the Class, never provided written consent allowing Defendants to capture, store, or disseminate his facial biometrics. Indeed, Defendants never presented Plaintiff any sort of prompt asking for his consent to gather his facial biometrics or providing him any of the disclosures required under BIPA to gather biometric identifiers.

39. Nor did Defendants have a publicly available policy at that time regarding their practices for collection, storage, retention period, or deletion of the facial biometrics they collected from property applicants like Plaintiff and the other members of the Class.

40. Plaintiff, like the other Class members, to this day does not know the whereabouts of his facial biometrics which Defendants obtained.

CLASS ALLEGATIONS

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

> **Class**: All individuals whose facial biometric identifiers or biometric information were collected, captured, stored, transmitted, disseminated, or otherwise used by Defendants within the state of Illinois from March 2018 to December 1, 2022.

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

43. There are 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 easily identified through Defendants' and their agents' records.

44. Plaintiff's claims are typical of the claims of the Class he seeks to represent, because the basis of Defendants' liability to Plaintiff and the Class is substantially the same, and because Defendants' conduct has resulted in similar injuries to Plaintiff and to the Class.

45. There are many questions of law and fact common to the claims of Plaintiff and the Class, 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 Defendants collect, capture, or otherwise obtain facial biometric identifiers or biometric information from Illinois residents;

b. Whether Defendants disseminated facial biometrics;

c. Whether Defendants obtained a written release from the Class members before capturing, collecting, or otherwise obtaining their facial biometric identifiers or biometric information;

d. Whether Defendants' conduct violates BIPA;

e. Whether Defendants' BIPA violations are willful or reckless; and

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

46. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would thus 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.

47. 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.

48. Defendants have 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
Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*
Against Defendants
(On behalf of Plaintiff and the Class)

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

50. Defendant Checkpoint is a private entity under BIPA.

51. Defendant IDScan is a private entity under BIPA.

52. BIPA requires private entities, such as Defendants, 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. BIPA also requires that a private entity in possession of biometric identifiers and/or biometric information establish and maintain a publicly available retention policy. An entity which possesses biometric identifiers or information must 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)..

54. Plaintiff and the other Class members have had their "biometric identifiers," namely their facial geometry and face prints, collected, captured, or otherwise obtained by Defendants when Defendants scanned their government issued ID documents and a live picture of their face to obtain a geometric template of their face in real-time through Defendants' biometric verification system. 740 ILCS 14/10.

55. Each instance when Plaintiff and the other Class members had their facial biometrics extracted by Defendants' automated biometric verification system, Defendants captured, collected, stored, and/or used Plaintiff's and the other Class members' facial geometry and face print biometric identifiers without valid consent and without complying with and, thus, in violation of BIPA.

56. Defendants' practice with respect to capturing, collecting, storing, and using biometrics fails to comply with applicable BIPA requirements:

a. Defendants failed to provide a publicly available retention schedule detailing the length of time for which the biometrics are stored and/or guidelines for permanently destroying the biometrics they store, as required by 740 ILCS 14/15(a);

b. Defendants failed to inform Plaintiff and the members of the Class in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);

c. Defendants failed to inform Plaintiff and the Class in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

d. Defendants failed to inform Plaintiff and the Class in writing the specific length of term their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

e. Defendants failed to obtain a written release, as required by 740 ILCS 14/15(b)(3); and

f. Defendants disseminated Plaintiff's and the Class' facial biometrics amongst each other as well as with third-party providers such as data storage providers without their consent in violation of 740 ILCS 14/15(d).

57. Defendants profited from Plaintiff's and the other Class members' facial biometrics in violation of 740 ILCS 14/15(c) as they were paid by their customers to biometrically verify each property applicant's identity.

58. Defendants knew, or were reckless in not knowing, that the automated biometric verification system that they provided and operated and which thousands of Illinois residents interacted with, would be subject to the provisions of BIPA, yet failed to comply with the statute.

59. By capturing, collecting, storing, and using Plaintiff's and the Class' facial biometrics as described herein, Defendants denied Plaintiff and the Class their right to statutorily required information and violated their respective rights to biometric information privacy, as set forth in BIPA.

60. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of $1,000 for each negligent violation of BIPA. 740 ILCS 14/20(1)-(2).

61. Defendants' violations of BIPA, a statute that has been in effect since 2008, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with BIPA.

62. Accordingly, with respect to Count I, Plaintiff, individually and on behalf of the proposed Class, pray for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, respectfully request 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 Defendants' actions, as set forth herein, violate BIPA;

c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendants to comply with BIPA;

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(2);

e. Awarding statutory damages of $1,000 for each negligent violation of the BIPA, pursuant to 740 ILCS 14/20(1);

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: March 14, 2023

Respectfully Submitted,
NICHOLAS HEGER, individually and on behalf of similarly situated individuals

By: /s/ Eugene Y. Turin
One of Plaintiff's Attorneys

Eugene Y. Turin
Timothy P. Kingsbury
MCGUIRE LAW, P.C. (Firm ID: 56618)
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Tel: (312) 893-7002
eturin@mcgpc.com
tkingsbury@mcgpc.com

Attorneys for Plaintiff and the Putative Class