

YES NO

EXHIBITS

CASE NO. 2021 CH 374

DATE: 1/26/2021

CASE TYPE: Class Action

PAGE COUNT: 15

CASE NOTE

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

MICHELLE CAMPANA, individually)
and on behalf of similarly situated)
individuals,)

Plaintiff,)

v.)

NUANCE COMMUNICATIONS, INC.,)
a Massachusetts Corporation.)

Defendant.)

No. 2021CH00374

Hon.

Jury Trial Demanded

11975810

CLASS ACTION COMPLAINT

Plaintiff Michelle Campana (“Plaintiff”), individually and on behalf of other similarly situated individuals, brings this Class Action Complaint against Defendant Nuance Communications, Inc. (“Nuance”) for violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”), and to obtain redress for all persons injured by Defendant’s conduct. Plaintiff alleges as follows based personal on knowledge as to her own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by her attorneys.

INTRODUCTION

1. Plaintiff seeks to represent a class of individuals who made one or more phone calls to entities who use automated interactive customer service phone software offered by Nuance Communications, Inc., and had their unique, biometric voiceprints collected and used without their consent or authorization.

2. Plaintiff and the other members of the putative class have suffered a concrete injury resulting from their voiceprint biometrics being collected, disseminated, and used for profit

FILED DATE: 1/26/2021 2:34 PM 2021CH00374

without their knowledge or consent, thus materially decreasing the security of this intrinsically inalterable information, and substantially increasing the likelihood that they will suffer as victims of fraud and/or identity theft in the future.

3. On behalf of herself and the proposed Class defined below, Plaintiff seeks an injunction requiring Defendant to comply with BIPA, as well as an award of statutory damages to the Class, together with costs and reasonable attorneys' fees.

PARTIES

4. At all relevant times, Plaintiff Michelle Campana has been a resident and a citizen of the state of Illinois.

5. Defendant Nuance Communications, Inc. is a Delaware company that conducts substantial business throughout Illinois, including in Cook County, and is registered with and authorized by the Illinois Secretary of State to transact business in Cook County, Illinois.

JURISDICTION AND VENUE

6. 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 doing business within this State and because Plaintiff's claims arise out of Defendant's unlawful in-state actions, as Defendant captured, collected, stored, used and profited from Plaintiff's biometric identifiers and/or biometric information in this State.

7. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101, because Defendant is doing business in Cook County and thus resides there under § 2-102.

THE BIOMETRIC INFORMATION PROTECTION ACT

8. “Biometrics” refers to a “biology-based set[s] of measurements.” *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017). Specifically, “biometrics” are “a set of measurements of a specified physical component (eye, finger, voice, hand, face).” *Id.* at 1296.

9. BIPA was enacted in 2008 in order to safeguard individuals’ biometrics as the result of the “very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information.” Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA is codified as Act 14 in Chapter 740 of the Illinois Compiled Statutes.

10. As set forth in BIPA, biologically unique identifiers, such as a person’s unique voiceprint, cannot be changed. 740 ILCS 14/5(c). The inalterable nature of biologically unique identifiers presents a heightened risk when an individual’s biometrics are not protected in a secure and transparent fashion. 740 ILCS 14/5(d)–(g).

11. As a result of the need for enhanced protection of biometrics, BIPA imposes various requirements on private entities that collect or maintain individuals’ biometrics, including voiceprints.

12. Among other things, BIPA seeks to regulate “the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.” 740 ILCS 14/5(g). BIPA thus applies to entities that interact with two forms of biometrics: biometric “identifiers” and biometric “information.” 740 ILCS 14/15(a)–(e).

13. BIPA defines a “biometric identifier” as any personal feature that is unique to an individual, including fingerprints, voiceprints, and hand geometry. “Biometric identifiers” are physiological, as opposed to behavioral, characteristics. BIPA’s text provides a non-exclusive list

of protected “biometric identifiers,” including “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10.

14. “Biometric information” is defined by BIPA 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.” *Id.* This definition helps ensure that information based on a biometric identifier that can be used to identify a person is covered by BIPA. Collectively, biometric identifiers and biometric information are known as “biometrics.”

15. In BIPA, the Illinois General Assembly identified four distinct activities that may subject private entities to liability:

- a. possessing biometrics without a proper policy publicly available, 740 ILCS 14/15(a);
- b. collecting biometrics, 740 ILCS 14/15(b);
- c. profiting from biometrics, 740 ILCS 14/15(c); and
- d. disclosing biometrics, 740 ILCS 14/15(d).

16. As the Illinois Supreme Court has held, BIPA “codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information.” *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206 (Ill. 2019). The Illinois Supreme Court further held that when a private entity fails to comply with BIPA “that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach.” *Id.*

A. Collecting Biometrics Under Section 15(b) of BIPA.

17. BIPA imposes three requirements that must be satisfied before any private entity may “collect, capture . . . or otherwise obtain” an individual’s biometrics:

- a. First, the private entity must inform the individual in writing that the

individual's biometrics are being collected or stored. 740 ILCS 14/15(b)(1).

- b. Second, the private entity must inform the individual in writing of the purpose and length of time for which their biometrics are being collected, stored, and used. 740 ILCS 14/15(b)(2).
- c. Finally, the private entity must receive a written release executed by the individual or a legally authorized representative. 740 ILCS 14/15(b)(3).

18. BIPA defines a "written release," outside the employment context, to mean "informed written consent." 740 ILCS 14/10.

B. BIPA's Unqualified Prohibition on Profiting from Biometrics Under Section 15(c).

19. BIPA additionally bars private entities from profiting from individuals' biometrics.

Section 15(c) provides as follows:

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.

740 ILCS 14/15(c).

20. Section 15(c) is an unqualified prohibition on profiting from biometrics.

C. Disseminating Biometrics Under Section 15(d).

21. BIPA also prohibits the "disclos[ure], redisclos[ure], or other[] disseminat[ion]" of biometrics without consent, unless the "disclosure or redisclosure completes a financial transaction" that is requested or authorized by the individual, is required by law, or is required in order to comply with a valid warrant or subpoena. 740 ILCS 14/15(d).

FACTUAL BACKGROUND

22. Defendant Nuance Communications, Inc. provides a number of voice data related products and services to hundreds of companies across the country that interact with thousands of Illinois residents daily. Defendant's products and services revolve around the integration of speech and voice recognition technology that utilize and rely on voiceprint biometrics.

23. Nuance has been providing voiceprint biometric services since 2001, and has integrated its voice biometric technology across a variety of services and platforms. Indeed, as part of its voiceprint biometrics services Nuance maintains one of the largest databases of voiceprints, containing 600 million voiceprints which Nuance uses to authenticate over 8 billion transactions a year.¹

24. A significant portion of the voiceprint biometric services provided by Nuance is its "Interactive Voice Response" ("IVR") software.

25. IVR is the robot voice that a caller hears when calling a customer support hotline. Nuance's IVR differs from traditional IVR because unlike traditional IVRs, Nuance's IVR software collects and analyzes callers' actual voiceprints to understand the caller's request and automatically respond with a personalized response instead of simply providing menus of options from which the caller can press a number to select what they wish to accomplish.²

26. By collecting individuals' unique voiceprints, Nuance's IVR software also allows its customers to trace every contact point, or "channel" as Nuance terms it, where a *specific* individual interacts with it. Thus, for example, when a caller contacts a customer service hotline that utilizes Nuance's IVR, the IVR software can extract the voiceprint of the caller to (1) track

¹ <https://investors.nuance.com/2020-09-03-Nuance-Named-Top-Biometrics-Vendor-by-Opus-Research-in-Intelligent-Authentication-and-Fraud-Prevention-Report> (accessed 1/19/2021).

² www.youtube.com/watch?v=Le5aEq-wqhg (accessed 1/19/2020).

the interaction, and (2) identify whether that individual has previously interacted with the company and through which means of contact the interaction occurred.

27. Nuance's IVR software also allows its customers to utilize its voiceprint identification functionality to try to identify individuals who may be engaging in fraudulent conduct by detecting specific speech patterns.³

28. While thousands of individuals across the country, and throughout Illinois, interact with Nuance's IVR software on a daily basis, Nuance fails to implement any sort of uniform policy to ensure that it obtains written consent from individuals interacting with its IVR software before obtaining their voiceprint biometrics.

29. For example, one of Nuance's biggest users of its IVR software is FedEx.

30. FedEx is one of the largest mail couriers in the world, averaging more than 16,000,000 packages processed and over 500,000 calls received every day.⁴

31. To help achieve customer service goals and reduce call agent volumes, FedEx, like numerous other Nuance customers, purchased access to Nuance's IVR software to create an automated interactive customer service phone line.⁵

32. When a caller calls FedEx's customer service phone line, as with other companies' utilizing Nuance's IVR software, they are greeted with an automated voice that asks the customer what they are calling about instead of simply presenting a predetermined set of options.

³ www.globenewswire.com/news-release/2018/02/26/1387271/0/en/Nuance-Introduces-Significant-Advancements-to-Market-Leading-Biometrics-Solution-Security-Suite-Leverages-AI-to-Curb-Fraud-Across-Voice-and-Digital-Channels.html (accessed 1/19/2020).

⁴ www.fedex.com/ma/about/overview/innovation.html (accessed 1/19/2021).

⁵ www.nuance.com/omni-channel-customer-engagement/case-studies/fedex.html (accessed on 1/19/2021).

33. To provide this “personalized” interactive voice experience to callers, Nuance’s IVR software uses its proprietary integrated artificial intelligence technology to collect and analyze the caller’s voiceprint so that it can determine the caller’s “intent,” understand the “context” of any requests made such as “scheduling a pickup” or “tracking a package,” and where appropriate route the call to the correct customer service department.⁶

34. Not only does Nuance’s IVR software collect and analyze callers’ voiceprints so that it can interact with them and understand their requests, but it also captures the data obtained and stores it so that it could be provided to a customer service agent if the caller is eventually transferred.⁷

35. Furthermore, as with its IVR software provided to other companies, the IVR software provided by Nuance to FedEx also incorporates “end-to-end” analytics that automatically captures every single call placed to the automated customer service phone line and analyzes the caller’s voiceprint to determine caller “intent,” create a transcript of any interaction and/or information provided, and even isolate the caller’s voice from any other audio that may be present during the call.⁸ This information is then provided to FedEx, as with other users of Nuance’s IVR software, so that FedEx can resolve any issues with customer interactions and determine whether the IVR software needs to be updated in any way to better respond to callers.

⁶ See www.nuance.com/omni-channel-customer-engagement/technologies/natural-language-understanding.html (accessed on 1/19/2021); www.nuance.com/content/dam/nuance/en_us/collateral/enterprise/data-sheet/ds-nuance-recognizer11-en-us.pdf (accessed on 1/19/2021); www.nuance.com/omni-channel-customer-engagement/voice-and-ivr/conversational-ivr.html (accessed on 1/19/2021);

www.nuance.com/omni-channel-customer-engagement/case-studies/fedex.html
⁷ www.nuance.com/omni-channel-customer-engagement/case-studies/fedex.html.

⁸ www.nuance.com/omni-channel-customer-engagement/case-studies/fedex.html;
www.nuance.com/omni-channel-customer-engagement/analytics/nuance-analytics.html
(accessed on 1/19/2021); www.nuance.com/omni-channel-customer-engagement/voice-and-ivr/insights.html (accessed on 1/19/2021).

36. Like thousands of other Illinois residents, Plaintiff interacted with Nuance's IVR software and had her voiceprint biometrics collected when she called FedEx's automated customer service phone line in late December 2020 to find out the status of a package that had been shipped to her.

37. When Plaintiff called FedEx's customer service phone line she was greeted by a recording which stated that the audio may be recorded for quality assurance, followed by an automated voice generated by Nuance's IVR software asking how it could assist Plaintiff.

38. Plaintiff interacted with Nuance's IVR software and asked for the status of a package shipment that she was scheduled to receive but had not arrived on time. Plaintiff was then prompted by the IVR software to provide tracking information. Plaintiff did not have the tracking information available at the time and requested that the IVR software transfer her to a customer service agent. Nuance's IVR software subsequently transferred Plaintiff to a FedEx customer service agent who provided Plaintiff additional information.

39. As with the thousands of other putative class members, from the moment that Plaintiff interacted and spoke to Nuance's IVR, her unique voiceprint was obtained to analyze Plaintiff's intent, determine the context of her call, prepare information to be passed on to the customer service representative, and to allow FedEx to review the phone call to determine whether there were any issues, errors, or misunderstandings made by Nuance's IVR.

40. However, at no point in time either before the call or during the call was Plaintiff aware that throughout the entire call Nuance's IVR software was collecting, analyzing, and storing her unique individual voiceprint as she interacted with the IVR system.

41. Nor did Plaintiff, like the thousands of Illinois residents who interact with Nuance's IVR software ever provide written consent allowing Nuance to capture, store, or disseminate her voiceprint biometrics.

42. Plaintiff to this day does not know the whereabouts of the voiceprint biometrics Nuance obtained from her through its IVR software.

CLASS ALLEGATIONS

43. Plaintiff brings this action on behalf of herself and a class of similarly situated individuals pursuant to 735 ILCS § 5/2-801. Plaintiff seeks to represent a Class (unless otherwise noted, "Class") defined as follows:

Class: All individuals whose voiceprint biometric identifiers or biometric information were collected, captured, stored, transmitted, disseminated, or otherwise used by or on behalf of Defendant within the state of Illinois any time within the applicable limitations period and for whom Defendant did not have any written record of consent to do so.

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 of such officer or director.

45. 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 Defendant's records, and records maintained by Defendant's customers.

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

47. 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 Defendant collects, captures, or otherwise obtains voiceprint biometric identifiers or biometric information from Illinois residents who interact with its IVR software;
- b. Whether Defendant disseminated voiceprint biometrics;
- c. Whether Defendant obtained a written release from the Class members before capturing, collecting, or otherwise obtaining their voiceprint biometric identifiers or biometric information;
- d. Whether Defendant's conduct violates BIPA;
- e. Whether Defendant's BIPA violations are willful or reckless; and
- f. Whether Plaintiff and the Class 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 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.

49. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class she seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her 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 her counsel has 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
Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq.
(On behalf of Plaintiff and the Class)

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

52. Defendant Nuance is a private entity under BIPA.

53. BIPA requires a private entity, 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).

54. Plaintiff and the other Class members have had their “biometric identifiers,” namely their voiceprints, collected, captured, or otherwise obtained by Defendant when they interacted with its IVR software. 740 ILCS 14/10.

55. Each instance when Plaintiff and the other Class members interacted with Defendant's IVR software, Defendant captured, collected, stored, and/or used Plaintiff's and the other Class members' voiceprint biometric identifiers without valid consent and without complying with and, thus, in violation of BIPA.

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

- a. Defendant 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);
- b. Defendant 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);
- c. Defendant 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);
- d. Defendant failed to obtain a written release, as required by 740 ILCS 14/15(b)(3);
and
- e. Defendant failed to obtain informed consent to disclose or disseminate the Class' biometrics to its customers such as FedEx, as required by 740 ILCS 14/15(d)(1).

57. By providing paying customers IVR software which uses voiceprint biometrics to analyze callers' voices and interact with them without any of the privacy protections required by BIPA, Defendant profited from Plaintiff's and the other Class members' voiceprint biometric identifiers in violation of 740 ILCS 14/15(c).

58. Defendant knew, or was reckless in not knowing, that the IVR software that it 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, using, and disseminating Plaintiff's and the Class' biometrics as described herein, Defendant 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. Defendant's 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, prays for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself 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 BIPA;
- c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendant 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: January 26, 2021

Respectfully Submitted,

MICHELLE CAMPANA, individually and on behalf of a class of similarly situated individuals

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

Eugene Y. Turin
Timothy P. Kingsbury
David Gerbie
Colin P. Buscarini
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
dgerbie@mcgpc.com
cbuscarini@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: [Nuance Communications Collected Customer Voiceprints in Violation of Ill. Privacy Law, Class Action Claims](#)
