FILED DATE: 10/10/2019 5:55 PM   2019CH11771

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

Deborah Zaluda, on her own behalf and on behalf of all others similarly situated

Plaintiff

v.

Apple Inc.

Defendant

No. `_____

2019CH11771

Hearing Date: 2/10/2020 10:00 AM - 10:00 AM
Courtroom Number: 2510
Location: District 1 Court
        Cook County, IL

## CHANCERY DIVISION CIVIL COVER SHEET
## GENERAL CHANCERY SECTION

A Chancery Division Civil Cover Sheet - General Chancery Section shall be filed with the initial complaint in all actions filed in the General Chancery Section of Chancery Division.  The information contained herein is for administrative purposes only.  Please check the box in front of the appropriate category which best characterizes your action being filed.

0005 ☐ Administrative Review
0001 ☑ Class Action
0002 ☐ Declaratory Judgment
0004 ☐ Injunction

0007 ☐ General Chancery
0010 ☐ Accounting
0011 ☐ Arbitration
0012 ☐ Certiorari
0013 ☐ Dissolution of Corporation
0014 ☐ Dissolution of Partnership
0015 ☐ Equitable Lien
0016 ☐ Interpleader
0017 ☐ Mandamus
0018 ☐ Ne Exeat

0019 ☐ Partition
0020 ☐ Quiet Title
0021 ☐ Quo Warranto
0022 ☐ Redemption Rights
0023 ☐ Reformation of a Contract
0024 ☐ Rescission of a Contract
0025 ☐ Specific Performance
0026 ☐ Trust Construction
    ☐ Other (specify) _____

By: /s/Daniel M. Feeney _____
☑ Atty. No.: 90236_____ ☐ Pro se 99500
Name: Miller Shakman Levine & Feldman LLP
Atty. for: Plaintiff
Address: 180 N. LaSalle St., Suite 3600
City/State/Zip: Chicago, IL  60601
Telephone: 312.263.3700
Primary Email: dfeeney@millershakman.com
Secondary Email: zfreeman@millershakman.com
Tertiary Email: odom@millershakman.com

**Pro Se Only:** ☐ I have read and agree to the terms of the *Clerk's Office Electronic Notice Policy* and choose to opt in to electronic notice from the **Clerk's Office** for this case at this Email address:

_____

**DOROTHY BROWN, CLERK OF THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS**

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

| | | |
|---|---|---|
| DEBORAH ZALUDA, individually and on behalf of all others similarly situated, | ) ) ) | |
| Plaintiff, | ) ) | No. **2019CH11771** |
| v. | ) ) | |
| APPLE INC., | ) ) | JURY TRIAL DEMANDED |
| Defendant. | ) ) ) ) | Hearing Date: 2/10/2020 10:00 AM - 10:00 AM Courtroom Number: 2510 Location: District 1 Court Cook County, IL |

## CLASS ACTION COMPLAINT

Plaintiff Deborah Zaluda ("Zaluda" or "Plaintiff"), individually and on behalf of all others similarly situated (the "Class"), brings the following Class Action Complaint pursuant to Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against Apple Inc. ("Apple" or "Defendant") to redress and curtail Defendant's unlawful collection, capture, use, and storage of Plaintiff's biometric data. Plaintiff alleges upon knowledge as to herself and her own acts and experiences, and upon the investigation of counsel, and upon information and belief as to all other matters against Defendant as follows:

## NATURE OF THE ACTION

1. This action arises from Defendant's unlawful collection, capture, retention, and disclosure of individuals' biometric information from approximately September 19, 2014 to the present (the "Class Period) in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/, *et seq.*

2. Apple is a leading technology company that designs and manufactures internet technology devices used by consumers worldwide. Apple designs and manufactures smartphones (iPhone), tablet computers (iPads), wearable technology (Apple Watch), laptop computers

(MacBook), desktop computers (iMac), and more. Apple also designs and develops software, including operating systems and other programs for each of its devices.

3.      Siri is an artificial intelligence-driven software program developed by Apple that allows individuals to, *inter alia*, use their voice to retrieve information from the internet, interact with internet-connected devices ("Smart Devices"), place calls, send texts, and schedule reminders. Apple preloads Siri on devices it designs and manufactures, including Apple's iPhone smartphones, iPad tablets, Apple Watches, AirPod headphones, HomePod smart speakers, MacBook laptops, and iMac computers ("Siri Devices").

4.      Before an individual can use a Siri Device, Siri asks the user to repeat a set of five phrases. Siri records the individual as she or he utters the phrases and analyzes the unique features of the speaker's voice. Apple calls this process "User Enrollment." Siri also records and analyzes the user's first forty requests in the same way and stores the resulting data. Apple refers to this dataset as a "User Profile." These User Profiles are voiceprints.

5.      The Illinois Biometric Information Privacy Act, 740 ILCS 14/, *et seq.* ("BIPA") regulates the collection, capture, retention, and dissemination of biometric identifiers and biometric information by private entities such as Apple. Pursuant to BIPA, biometric identifiers specifically include voiceprints. Biometric information is defined by BIPA as information based on an individual's biometric identifier used to identify an individual.

6.      BIPA prohibits a private entity such as Apple from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining an individual's biometric information or biometric identifier unless it first:

> (1) Informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

2

(2) Informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) Receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

7.      BIPA also prohibits private entities from sharing an individual's biometric identifier or biometric information unless:

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

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

(3) The disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) The disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

8.      BIPA also requires companies in possession of biometric identifiers or biometric information to develop and make available to the public a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Private entities are required by BIPA to comply with such written policy.

9.      Apple collects, captures, stores and disseminates voiceprints of each individual who uses Siri. Apple does not inform Siri users prior to or after User Enrollment that it will

capture, collect, store, and/or disseminate their voiceprints, and does not obtain Siri user consent to such capture, collection and storage of their voiceprints, as BIPA requires.

10.    Additionally, Apple has not developed or made available to the public or implemented and complied with a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first, in violation of BIPA.

11.    Accordingly, Plaintiff, on behalf of herself as well as the putative Class, seeks an order: (1) declaring that Apple's conduct violates BIPA; (2) requiring Apple to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

12.    Given the concealed and secretive nature of Apple's conduct, more evidence supporting the allegations in this complaint will be uncovered after a reasonable opportunity for discovery.

### JURISDICTION AND VENUE

13.    This Court has jurisdiction over Apple pursuant to 735 ILCS § 5/2-209 because Apple conducts business in Illinois, committed the statutory violations alleged herein in Cook County and throughout Illinois, and is registered to and does conduct business in Illinois.

14.    Venue is proper in Cook County because Apple conducts business in this State, conducts business in Cook County, and committed the statutory violations alleged herein in Cook County and throughout Illinois.

4

**PARTIES**

**A. Plaintiff**

15. Plaintiff Deborah Zaluda is a natural person and is a resident and citizen of the

State of Illinois.

**B. Defendant**

16. Defendant Apple Inc. is a business incorporated under the laws of the State of

Delaware with its principal place of business in Cupertino, California. At all times mentioned

herein, Apple has been engaged in the State of Illinois in the business of designing,

manufacturing, distributing, and selling, *inter alia,* smartphones, tablet computers, wearable

computers, headphones, laptops, and desktop computers that come with software Apple develops

pre-installed.

**FACTUAL BACKGROUND**

**I. Biometric Identifiers and Biometric Data**

17. Biometrics is the measurement and analysis of unique physical or behavior

characteristics. Biometric data is frequently used to identify individuals, for example through the

use of fingerprint scans, facial recognition, or voice patterns. A dataset that corresponds to a

person's unique physical or behavioral characteristic that is used for identification purposes,

(*e.g.,* data corresponding to a fingerprint, voice pattern, retina, or facial features) is commonly

referred to as a "biometric identifier."

18. Despite consumers' ever-growing concerns with privacy, the use of biometric

data by private companies is accelerating, with much of this growth attributable to the increased

capability of smartphones and other internet-connected devices to capture and collect an

individual's biometric data.

5

19.     Since an individual's physical characteristics cannot be easily changed (if at all), the use of biometric identifiers has serious implications for an individual's privacy. An entity that obtains possession of an individual's biometric identifier is able to track that individual wherever a device capable of capturing biometric identifiers is present. Additionally, because many financial institutions and healthcare providers use biometric identifiers for authentication, possession of a person's biometric identifier can provide access to an individual's bank accounts or medical records.

## II.     The Illinois Biometric Information Privacy Act

20.     In recognition of the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information[,]"[1] the Illinois General Assembly passed the Biometric Information Privacy Act, 740 ILCS 14/ ("BIPA") in 2008.  Because biometric identifiers cannot be changed if they are compromised or misused, the General Assembly has provided citizens of Illinois, through the protections afforded by BIPA, the ability – and statutory right – to control their biometric identifiers and biometric information by requiring private companies to obtain their consent before creating and collecting such identifiers and information, including the right to prevent such creation and collection by refusing to withholding consent.

21.     In enacting BIPA, the General Assembly recognized that the full extent of the damage that can result from the compromise or misuse of an individual's biometric data cannot be ascertained in advance. The General Assembly thus sought to head off such problems before they occur by imposing safeguards to protect individuals' privacy rights in their biometric identifiers and biometric information.

---

[1] Illinois House Transcript 2008 Reg. Sess. No. 276.

22.    BIPA ensures that individuals' privacy rights in their biometric identifiers and biometric information are protected by making it unlawful for a private company to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

> (l) 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 term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."[2]

23.    BIPA's definition of "biometric identifiers" expressly includes a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[3]

24.    BIPA further protects consumer's right to privacy in their biometric identifiers and biometric information by making it unlawful for a private entity to "disclose, redisclose, or otherwise disseminate" an individual's biometric identifier and/or and biometric information unless:

> (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
>
> (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
>
> (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

---

[2] 740 ILCS 14/15 (b).

[3] 740 ILCS 14/10 (emphasis added).

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.[4]

25.     BIPA further requires private entities in possession of biometric identifiers or biometric information to:

> develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.[5]

26.     BIPA further provides that, absent a valid warrant or subpoena, a private entity in possession of biometric identifiers or biometric information "must comply with its established retention schedule and destruction guidelines.[6]

27.     The General Assembly intended the relief provided to aggrieved individual to have substantial force by subjecting private entities that fail to comply with BIPA to liability, including liquidated damages, to prevent unforeseen problems that cannot be undone before they occur. Thus, private entities that fail to adhere to the safeguards imposed by BIPA are subject to liquidated damages, injunctions, attorneys' fees, and litigation expenses for each violation of BIPA.[7]   In particular, BIPA provides for statutory damages for each violation as follows:

> (1) $1,000 or actual damages, whichever is greater, for negligent violations; or
>
> (2) $5,000 or actual damages, whichever is greater, for intentional or reckless violations.[8]

---

[4] 740 ILCS 14/15 (d).

[5] 740 ILCS 14/15 (a).

[6] *Id.*

[7] 740 ILCS 14/20.

[8] *Id.*

8

### III.     Apple and Siri

28.     Apple is an internet technology company that designs and manufactures consumer devices used by billions of consumers worldwide. Apple designs, manufactures, and sells computer technology such as smart phones (iPhone), tablet computers, (iPad), smart speakers (HomePod), music players (iPod), laptops (MacBook), desktop computers (iMac), wearable devices (Apple Watch), headphones (AirPods), and more.

29.     Apple also develops operating system software for their consumer devices, including: iOS (iPhone, iPad, and iPod), watchOS (Apple Watch), macOS (iMac and MacBook), tvOS (Apple TV), and audioOS (HomePod). Each of these operating systems includes a feature known as Siri.

30.     Siri is a voice-activated virtual person assistant feature that is included with devices running Apple operating systems iOS, watchOS, macOS, tvOS, and audioOS. Siri uses the internet to help users with a variety of tasks, including providing users with information in response to questions, play music, and interact with other internet-connected devices, among other things.

31.     Siri has been pre-installed on devices running iOS since October 12, 2011, but initially could only be used when the user pressed the device's home button. Apple introduced a voice-activated "wake" feature for Siri, utilizing a voice command, with the launch of iOS8 and the iPhone 6S on September 19, 2014. Today, Siri is an operating system feature on the following Apple devices: iPhone, iPad, iPod touch, AirPod headphones, CarPlay, Apple Watch, HomePod, Mac, MacBook, and Apple TV.

32.     Since September 19, 2014, users have activated Siri through the utterance of the pre-programmed wake phrase "Hey Siri" or by a physical gesture such as the pushing of the

9

home button or a wrist movement. In order to recognize the utterance of a wake phrase, Siri Devices' speech recognizer constantly records and analyzes short snippets of audio within range of the device's microphone and analyzes those clips to determine whether the wake phrase "Hey Siri" has been uttered ("Passive Listening").

33.     According to Apple, when a Siri Device is in Passive Listening mode, the short audio clips that are recorded are stored locally on the Siri Device's random-access memory ("RAM") to be analyzed. These snort snippets are continuously overwritten as a Siri Device analyzes new audio clips during Passive Listening.

34.     When a Siri Device determines "Hey Siri" has been uttered within range of its microphone, it "wakes up" or activates Siri. Once activated, Siri records an individual's speech to determine what Siri is being asked to do. These recordings are sent to Apple's servers for analysis to determine (1) whether the Siri Device accurately detected a wake phrase; and (2) confirm what Siri is being asked to do so Apple can respond to the command. For example, if a user says, "Hey Siri, what is the weather in Chicago?" Siri will transmit that audio to Apple for analysis. Apple analyzes audio by converting what is said into text so that Apple's computers can determine what is being requested. Users can also ask Siri to perform other tasks, such as set alarms, reminders, read text message aloud, or interact with other internet connected smart devices.

35.     The development of virtual assistants that record individuals' voices has raised numerous privacy concerns. For example, some individuals have voiced concerns that rather than only activating in response to a wake phrase, virtual assistants are always recording, resulting in the recording of personal and confidential communications.

10

36.     Apple has used its privacy practices as a marketing tool to distinguish itself from competitors such as Google, Amazon, and Facebook that have been implicated in collecting, exploiting, and sharing sensitive customer data. For example, Apple has put up billboards stating "What happens on your iPhone stays on your iPhone." Apple's CEO Tim Cook has commented that Apple "believes privacy is a human right," and that "we also recognize that not everyone sees things as we do."[9]

37.     Despite positioning itself as a privacy leader, Apple – along with Amazon, Google, Facebook, and Microsoft – was recently revealed to have shared recordings made by Siri with contractors who then listened to the conversations for purposes of evaluating Siri's performance.[10] The contractors regularly heard conversations where no wake phrase was uttered. These conversations included "private discussions between doctors and patients, business deals, seemingly criminal dealings, sexual encounters and so on."[11] These recordings were accompanied by user data showing location, contact details, app data, and more, which could allow contractors to identify the users they were listening to. Apple had represented that any recordings made by Siri were completely anonymized.

38.     On information and belief, Apple has disclosed biometric information to third parties about Plaintiff and the Class members.

---

[9] Ian Bogost, *Apple's Empty Grandstanding About Privacy: The company enables the surveillance that supposedly offends its values,* The Atlantic, Jan. 31, 2019, https://www.theatlantic.com/technology/archive/2019/01/apples-hypocritical-defense-data-privacy/581680/ (last accessed Oct. 8, 2019).

[10] Alex Hern, *Apple contractors 'regularly hear confidential details on Siri recordings,* The Guardian, July 26, 2019, https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings (last accessed Oct. 8, 2019).

[11] *Id.*

11

## SUBSTANTIVE ALLEGATIONS

**I.    Apple is Capturing, Collecting, and Disclosing Consumers' Voiceprints without Consent.**

39.    In developing Siri, Apple focused on developing software capable of *speech* recognition (to recognize the key phrase "Hey Siri") and *speaker* recognition (to recognize that the individual speaking is someone that has consented to be recorded).

40.    According to Apple, "[t]he overall goal of speaker recognition [] is to ascertain the identity of a person using his or her voice."[12] Speaker recognition is therefore interested in "who is speaking," as opposed to "what was spoken."[13] To give Siri speaker recognition capabilities, Apple developed a process it calls "User Enrollment." When an individual first attempts to use Siri on a Siri Device, the individual is asked to repeat the following five phrases:

1.    "Hey Siri"
2.    "Hey Siri"
3.    "Hey Siri"
4.    "Hey Siri, how is the weather today?"
5.    "Hey Siri, it's me."[14]

41.    According to Apple, "[t]hese phrases are used to create a statistical model for the user's voice"[15] through the following process: First, Siri "converts the incoming speech utterance to a fixed-length speech (super)vector, which can be seen as a summary of the acoustic information present in the 'Hey Siri' utterance; this includes information about the phonetic content, the background recording environment, *and the identity of the speaker* (emphasis added)."[16] Second, Siri "attempts to transform the speech vector in a way that focuses on

---

[12] *Personalized Hey Siri – Apple*, 1 Apple Machine Learning Journal 9, April 2018, at 4 (hereinafter "*Personalized Hey Siri*").

[13] *Id.*

[14] *Id.*

[15] *Id.* at 4.

[16] *Id.* at 6.

12

speaker-specific characteristics and deemphasizes variabilities attributed to phonetic and environmental factors."[17]

42.     Apple refers to the voice data captured and collected from the Siri User Enrollment as a "User Profile." User profiles are voiceprints, and Apple has collected, captured, and stored the voiceprints of millions of Illinois consumers without acquiring informed consent in accordance with BIPA.

43.     BIPA requires Apple to obtain informed consent from Siri users in writing *before it* collects an individual's voiceprint. But, contrary to BIPA, nowhere in Apple's terms of service, privacy policy, or other disclosures does Apple state it is collecting an individual's biometric identifier, biometric information, or voiceprint. This runs afoul of the intention of the Illinois General Assembly in enacting BIPA: to require private companies to explicitly state they are collecting biometric identifiers and biometric information before doing so, so that consumers can make informed decisions about whether to enter into transaction with the companies or use the companies' products.

44.     BIPA also requires Apple to obtain Siri users' informed written consent before disclosing, redisclosing, or otherwise disseminating biometric identifiers and/or biometric information. According to published reports, Apple has disclosed, redisclosed, or otherwise disseminated user data affiliated with voiceprints to third party contractors.[18] Nowhere in its terms of service, privacy policy, or other disclosures has Apple given Siri users notice of such disclosures.

---

[17] *Id.*

[18] Alex Hern, *Apple contractors 'regularly hear confidential details on Siri recordings,* The Guardian, July 26, 2019, https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings (last accessed Oct. 8, 2019).

13

**II.** **Apple Collected, Captured, and Stored Plaintiff's Biometric Identifier or Biometric Information without Consent**

45. For a number of years prior hereto and to the present time, Plaintiff Deborah Zaluda has owned and used a number of Apple Devices with the Siri function, including Apple iPhones, an Apple Watch and two Apple iMac computers. At the present time (and since 2018), Plaintiff has owned and used an Apple iPhone XS with a Siri function.

46. At all times mentioned herein, Plaintiff Deborah Zaluda has been a Siri user and underwent Siri's User Enrollment and has used the Siri function on her Apple Devices. Siri has recorded her initial (User Enrollment) utterances, and subsequent utterances, analyzed them, created a statistical model of Plaintiff's voice, and collected, captured and stored a voiceprint of Plaintiff's voice.

47. At no point did Plaintiff have knowledge that Apple was creating and capturing a voiceprint of her voice and collecting and storing such voiceprint, At no point did Plaintiff consent to the unlawful collection, capture, and storage of her voiceprint. Apple did not inform Plaintiff in writing that it was collecting, capturing, and storing her biometric identifier or biometric information, Apple did not inform Plaintiff in writing of the specific purpose and length of term which her biometric identifier or biometric information was being collected, stored, and used, and Apple did not obtain a written release by which Plaintiff consented to the collection, capture, and storage of her biometric identifier and biometric information as required by BIPA.

48. At no point did Plaintiff consent to the unlawful disclosure, redisclosure, or dissemination of her biometric identifier or biometric information. Apple did not inform Plaintiff that it was disclosing, redisclosing, or otherwise disseminating her biometric identifier and/or biometric information.

14

49.     Apple unlawfully captured, collected and disclosed Plaintiff's biometric identifier and biometric information, without consent, in violation of BIPA.

50.     Additionally, Apple has not developed and made available to public, nor implemented and complied with a written policy outlining Apple's handling of Plaintiff's biometric identifiers and biometric information as required by BIPA, and has thus violated BIPA requirements that such a policy adopted and that Apple comply with the retention and destruction provisions of such policy.

## CLASS ACTION ALLEGATIONS

51.     Plaintiff brings this action pursuant the Illinois Code of Civil Procedure, 735 ILCS 5/2-801, on her own behalf and as a representative of all other similarly-situated individuals, defined as follows (the "Class"):

> All persons who used the Siri function on an Apple device in the State of Illinois and had their voiceprints collected, captured, received, or otherwise obtained and/or disseminated by Apple.[19]

52.     Excluded from the class is: (1) any Judge or Magistrate presiding over this action and any members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and their current and former employees, officers, and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

---

[19] Plaintiff has defined the Class based on currently available information and hereby reserves the right to amend the definition of the Class, including, without limitation, the Class Period.

15

53. This action is properly maintained as a class action under 735 ILCS 5/2-801 because: (1) the class is so numerous that joinder of all member is impracticable ("Numerosity"); (2) there are questions of law or fact that are common to the class ("Commonality"); (3) Plaintiff's claims are typical of the claims of the class ("Typicality"); and (4) Plaintiff will fairly and adequately protect the interest of the class ("Adequate Representation").

54. **Numerosity**. The Class likely consists of thousands, if not millions, of individuals, and the members can be identified through Apple's records. The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable.

55. **Predominant Common Questions**. The Class's claims present common questions of law and fact and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

 a. Whether Apple has collected, captured, or otherwise obtained, stored and/or disseminated Plaintiff's and the Class's biometric identifiers or biometric information;

 b. Whether Apple properly informed Plaintiff and the Class that it collected, captured, used, stored and/or disclosed their biometric identifiers or biometric information;

 c. Whether Apple obtained a written release (as defined in 740 ILCS 14/10) to collect, capture, use, store and/or disclose Plaintiff's and the Class's biometric identifiers or biometric information;

 d. Whether Apple developed, made available to the public, and complied with a written policy, establishing a retention schedule and guidelines for permanently destroying biometric identifiers or biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction, whichever comes first;

 e. Whether Apple used Plaintiff's and the Class's biometric identifiers or biometric information to identify them;

16

f.   Whether Apple's collection, capture, storage, and/or sharing of Plaintiff's and the Class's biometric identifiers or biometric information violated BIPA.

g.   Whether Apple's failure to develop, make available to the public, and comply with a written policy, establishing a retention schedule and guidelines for permanently destroying biometric identifiers or biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction, whichever comes first, violated BIPA; and

h.   Whether Apple's violations of BIPA were committed intentionally, recklessly, or negligently.

56.   **Typicality**. Plaintiff's claims are typical of the claims of the other members of the proposed Class. Plaintiff and Class members were aggrieved as a result of Apple's wrongful conduct that is uniform across the Class.

57.   **Adequate Representation**. Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel that is competent and experienced in complex litigation and class actions. Plaintiff has no interest that is antagonistic to those of the Class, and Apple has no defenses unique to Plaintiff. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor Plaintiff's counsel have any interest adverse to those of the other members of the Class.

58.   **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. It would be unduly burdensome to the Court for each class member to pursue their claims individually. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and

17

comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

59.     Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

## CLAIMS FOR RELIEF

## FIRST CLAIM FOR RELIEF

**Violation of the Illinois Biometric Information Privacy Act, 740 ILCS § 14/15(b)**
**Failure to Obtain Informed Written Consent and Release before**
**Obtaining Biometric Identifiers or Biometric Information**
**(On Behalf of Plaintiff and the Class)**

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

61.     BIPA requires companies to obtain informed written consent from individuals before collecting or capturing their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a 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 term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS 14/15(b).

62.     Apple is a "private entit[y]" pursuant to 740 ILCS § 14/10.

63.     Plaintiff and the Class are individuals who have had their "biometric identifiers" (voiceprints) collected and captured by Apple.

18

64.     Plaintiff's and the Class's biometric identifiers were used to identify them and therefore constitute "biometric information" as defined by 740 ILCS § 14/10.

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

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

67.     By collecting, storing, and using Plaintiff's and the Class's biometric identifiers and/or biometric information as described herein, Apple violated Plaintiff's and the Class's rights to privacy in their biometric identifiers or biometric information.

68.     On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Apple to comply with BIPA's requirements for the collection, capture, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

**SECOND CLAIM FOR RELIEF**

**Violation of the Illinois Biometric Information Privacy Act, 740 ILCS § 14/15(d)**
**Failure to Obtain Consent before Disclosing, Redisclosing,**
**or otherwise Disseminating Biometric Identifiers or Biometric Information**
**(On Behalf of Plaintiff and the Class)**

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

70.     BIPA requires companies to obtain consent from individuals before disclosing,

redisclosing, or otherwise disseminating their biometric identifier and/or biometric information.

740 ILCS 14/15(d).Apple has used Plaintiff's and the Class's biometric identifiers to identify

them and such identifiers therefore constitute "biometric information" as defined by 740 ILCS §

14/10.

71.     Plaintiff and the Class are individuals who have had their "biometric identifiers"

(voiceprints) disclosed, redisclosed, or otherwise disseminated by Apple.

72.     Apple did not obtain consent from Plaintiff and the Class before disclosing,

redisclosing, or otherwise disseminating their biometric identifiers and/or biometric information

as required by 740 ILCS 14/15(d)(1).

73.     By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class's

biometric identifiers and/or biometric information as described herein, Apple violated BIPA.

74.     On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2)

injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by

requiring Apple to comply with BIPA's requirements for the collection, capture, storage, and use

of biometric identifiers and biometric information as described herein; (3) statutory damages of

$5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or,

in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to

740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

## THIRD CLAIM FOR RELIEF

**Violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/15(a)**
**Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule**

**(On Behalf of Plaintiff and the Class)**

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

76.     BIPA requires that private companies in possession of biometric identifiers and biometric information develop, make available to the public, and comply with a written policy setting forth a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

77.     Plaintiff and the Class are individuals who have had their "biometric identifiers" (voiceprints) collected and captured by Apple.

78.     Plaintiff's and the Class's biometric identifiers were used to identify them and therefore constitute "biometric information" as defined by 740 ILCS § 14/10.

79.     Apple systematically and automatically collected, captured, used, stored and disseminated Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

80.     Apple has failed to develop, make available to the public, and comply with a written policy setting forth retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and will not destroy Plaintiff's or the Class's biometric

21

data when the initial purpose for collecting or obtaining such data has been satisfied or within

three years of the individual's last interaction with the company, in violation of BIPA.

81.     On behalf of herself and the Class, Plaintiff seeks: (1) declaratory relief; (2)

injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by

requiring Apple to comply with BIPA's requirements for the collection, storage, and use of

biometric identifiers and biometric information as described herein; (3) statutory damages of

$5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or,

in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to

740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses

pursuant to 740 ILCS 14/20(3).

## **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff on behalf of herself and the proposed Class respectfully request

that the Court enter an order:

A.     Certifying this case as a class action on behalf of the Class defined above,

appointing Plaintiff Deborah Zaluda as Class Representative, and appointing Silver Golub &

Teitell LLP as Class Counsel;

B.     Declaring that Apple's actions, as set out above, violate BIPA;

C.     Awarding statutory damages of $5,000 for each intentional and /or reckless

violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of

$1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1);

D.     Declaring that Apple's actions, as set forth above, were intentional and/or

reckless;

E.      Awarding injunctive and other equitable relief as is necessary to protect the

interests of Plaintiff and the Class, including an Order requiring Apple to collect, store, use and

disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F.      Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and

other litigation expenses pursuant to 740 ILCS 14/20(3);

G.      Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent

allowable;

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

## DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated:  October 10, 2019                          Respectfully submitted,

                                                  DEBORAH ZALUDA

                                                  /s/ Daniel M. Feeney
                                                  One of her attorneys

Daniel M. Feeney
Zachary J. Freeman
Miller Shakman Levine & Feldman LLP
Firm ID: 90236
180 North LaSalle Street, Suite 3600
Chicago, IL 60601
Tel. (312) 263-3700
Fax. (312) 263-3270
Email: dfeeney@millershakman.com
        zfreeman@millershakman.com

David S. Golub (*pro hac vice* forthcoming)
Steven L. Bloch (*pro hac vice* forthcoming)
Ian W. Sloss (*pro hac vice* forthcoming)
Silver Golub & Teitell LLP
184 Atlantic Street
Stamford, CT 06901
Tel. (203) 325-4491

Fac. (203) 325-3769
Email:  dgolub@sgtlaw.com
      sbloch@sgtlaw.com
      isloss@sgtlaw.com

## SUPREME COURT RULE 222(b) DAMAGES AFFIDAVIT

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that this civil action seeks in excess of $50,000 on behalf of the Plaintiff and the proposed Class.

Dated: October 10, 2019

/s/ Daniel M. Feeney
One of Plaintiffs' attorneys

Daniel M. Feeney
Zachary J. Freeman
Miller Shakman Levine & Feldman LLP
Firm ID: 90236
180 North LaSalle Street, Suite 3600
Chicago, IL 60601
Tel. (312) 263-3700
Fax. (312) 263-3270
Email: dfeeney@millershakman.com
        zfreeman@millershakman.com

David S. Golub (*pro hac vice* forthcoming)
Steven L. Bloch (*pro hac vice* forthcoming)
Ian W. Sloss (*pro hac vice* forthcoming)
Silver Golub & Teitell LLP
184 Atlantic Street
Stamford, CT 06901
Tel. (203) 325-4491
Fac. (203) 325-3769
Email: dgolub@sgtlaw.com
        sbloch@sgtlaw.com
        isloss@sgtlaw.com