

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

THELTON GEORGE PARKER, JR. AND
STEVEN DOYLE, Individually and on Behalf of
All Others Similarly Situated,

Plaintiffs,

v.

VERIZON COMMUNICATIONS INC. AND CELLCO
PARTNERSHIP D/B/A VERIZON WIRELESS,

Defendants.

Case No.: 24-cv-8436

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Thelton George Parker, Jr. (“Mr. Parker”) and Steven Doyle (“Mr. Doyle”) (together, “Plaintiffs”), individually and on behalf of all others similarly situated (collectively, the “Class,” as more fully defined below), bring this Class Action Complaint against Verizon Communications Inc. (“Verizon”) and Cellco Partnership d/b/a Verizon Wireless (“Verizon Wireless”) (together, “Defendants”) for their violations of the Illinois Biometric Privacy Act, 740 ILCS 14/1, *et seq.* (“BIPA”), and to obtain redress for all persons injured by Defendants’ conduct. Plaintiffs allege as follows:

I. INTRODUCTION AND NATURE OF THE CASE

1. BIPA defines a “biometric identifier” as any personal feature that is unique to an individual, including a voiceprint. 740 ILCS 14/10. “Biometric information” is defined as any information based on a biometric identifier, regardless of how it is converted or stored. *Id.* Biometric identifiers and biometric information are collectively referred to herein as “biometrics.”

2. A voiceprint, which is an individually unique and distinctive pattern of certain voice characteristics that are used to identify a person, is comprised of, and uses, biometrics, and is expressly defined as a “biometric identifier” under BIPA.

3. The unique nature of biometrics allows private entities to utilize their customers’ biometrics for identification and authentication purposes, and many companies use biometrics for such purposes.

4. BIPA does not prohibit companies from using their customers’ biometrics in this fashion. In enacting BIPA, however, the Illinois General Assembly recognized that “biometrics are unlike other unique identifiers that are used to access finances or other sensitive information,” (740 ILCS 14/5), and therefore require special treatment compared to traditional private personally identifiable information. For example, even sensitive information like Social Security or driver’s license numbers, when compromised, can be changed. “Biometrics, however, are biologically unique to each individual; therefore, 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.

5. To address these risks, BIPA provides, *inter alia*, that private entities such as Defendants may not collect, capture, purchase, receive through trade, or otherwise obtain an individual’s biometrics, including a voiceprint, unless it first:

- a. informs that person in writing that biometrics will be collected or stored;
- b. informs that person in writing of the specific purpose and the length of term for which such biometrics are being collected, stored and used; and
- c. receives a written release from that person for the collection of their biometrics.

740 ILCS 14/15(b)(1)-(3).

6. Recognizing that typical consumers are not equipped to defend themselves from large corporations bent on acquiring and exploiting their most private, unchangeable information, the Illinois Legislature, by enacting BIPA, gives consumers a powerful, protective tool.

7. Despite BIPA's clear mandates, Defendants failed to make required disclosures regarding its collection, use, and storage of biometrics and did not obtain their customers' legally-required informed written consent prior to collecting their customers' voiceprints in connection with a service known as Voice ID.

8. Defendants describe Voice ID in multiple, sometimes contradictory, ways. But generally, Defendants purport that Voice ID authenticates the caller during phone calls with Defendants.

9. Defendants, however, failed to obtain the informed, written consent of their customers prior to collecting and using their voiceprints. Defendants never informed Voice ID users that their biometric identifiers and biometric information were being collected or stored—during the initial enrollment process or during subsequent phone calls while Voice ID was active and being used. Defendants also failed to inform customers of any specific purpose for the collection or storage of their biometric identifiers or biometric information, and failed to provide customers a schedule setting out the length of time during which those biometric identifiers or biometric information would be collected, stored, used, or destroyed.

10. Defendants are large, multibillion-dollar corporations which, upon information and belief, have access to lawyers (both in-house and outside counsel) to advise them on compliance with state privacy laws such as BIPA. Moreover, BIPA compliance (or lack thereof) has been the subject of significant litigation and legal commentary over the past decade-plus. Defendants'

violations of BIPA cannot be the result of oversight or lack of legal guidance, but are instead intentional and reckless, or at the very least negligent.

11. Defendants continue to violate BIPA each and every time a customer enrolls in Voice ID. As a result of Defendants' ongoing BIPA violations, Plaintiffs, individually and on behalf of the other Class members, ask the Court to impose upon Defendants the BIPA-mandated statutory damages relating to the collection, storage, and disclosure of Plaintiffs' biometric identifiers and/or biometric information, as well as injunctive relief requiring Defendants to comply with BIPA's strict mandates.

II. PARTIES

A. Plaintiffs

12. Mr. Parker is a resident of Oak Park, Illinois, where he intends to remain.

13. Mr. Doyle is a resident of Naperville, Illinois, where he intends to remain.

B. Defendants

14. Defendant Verizon Communications Inc. is a communications company that provides, among its business lines, consumer mobile phone service. Verizon Communications is a Delaware corporation and maintains its principal place of business at 1095 Avenue of the Americas, New York, New York 10036.

15. Defendant Cellco Partnership d/b/a Verizon Wireless is a Delaware entity, maintains its principal place of business at One Verizon Way, Basking Ridge, New Jersey 07920, and maintains a registered agent in this District at c/o CT Corporation System, 208 S. LaSalle Street, Suite 814, Chicago, Illinois 60604. Verizon Wireless is a wholly owned subsidiary of Verizon. Verizon provides cellular phone products and services through Verizon Wireless.

III. JURISDICTION AND VENUE

16. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332, because (a) this is a proposed class action in which there are at least 100 Class members; (b) the parties are minimally diverse, as Plaintiffs and Defendants are domiciled in different states; and (c) the combined claims of Class members exceed \$5,000,000, exclusive of interest, attorneys' fees, and costs.

17. This Court has personal jurisdiction over Defendants because Defendants regularly conduct business throughout Illinois, including the marketing and sale of its telecommunication services, including, but not limited to, and the marketing and use of Voice ID to consumers in Illinois.

18. Venue is also appropriate in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. BIPA's Legal Framework

19. In late 2007, a company called Pay By Touch, which provided major retailers throughout Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois General Assembly because suddenly a serious risk emerged that millions of fingerprint records—which are unique biometrics—could be linked to Illinois residents' sensitive financial and personal data and could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois residents. The bankruptcy also highlighted the fact that most consumers who had used that company's biometric scanners were completely unaware that the scanners were not actually transmitting data to the retailer who deployed the scanner, but rather to the now-bankrupt company, and that their unique biometrics could now be sold to unknown third parties.

20. Recognizing the “very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information,” the Illinois General Assembly enacted BIPA in 2008 to protect the privacy rights of every Illinois resident who has their unique, biometric identifiers captured or retained by self-interested, profit-obsessed companies. Ill. House Tr., 2008 Reg. Sess. No. 276; 750 ILCS 14/5.

21. In enacting BIPA, the General Assembly found that the sensitivity of biometric identifiers and/or biometric information warrants heightened protection because companies frequently collect it from individuals like Plaintiffs and the other Class members. Specifically, the General Assembly found that “[b]iometrics are unlike other unique identifiers” like Social Security Numbers because they are “biologically unique to the individual” and cannot be changed if compromised. 740 ILCS 14/5(c). Thus, a person whose biometrics are compromised “has no recourse” and “is at heightened risk for identity theft.” *Id.*

22. When enacting BIPA, the General Assembly recognized that “[t]he full ramifications of biometric technology are not fully known.” 740 ILCS 14/5(e). Therefore, “[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.” 740 ILCS 14/5(f).

23. BIPA defines “biometric identifiers” as “a retina or iris scan, fingerprint, **voiceprint**, or scan of hand or face geometry.” 740 ILCS 14/10 (emphasis added).

24. “Biometric information,” in turn, is identified 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.*

25. Accordingly, BIPA requires “private entities”—including companies like Verizon and Verizon Wireless—that collect certain biometric identifiers or biometric information, or cause such information and identifiers to be collected, to take a number of specific steps to safeguard the biometric data they collect, store, capture, or otherwise obtain.

26. BIPA is an informed consent statute. Thus, companies that collect biometric identifiers or biometric information, such as Verizon and Verizon Wireless, must obtain informed consent from consumers prior to collecting such data from them, and they must publicly disclose to consumers their uses, retention of, and schedule for destruction of the biometric information or identifiers that they do collect.

27. With respect to safeguarding biometrics, BIPA requires that private entities—including companies like Verizon and Verizon Wireless—that possess biometric identifiers or biometric information:

[D]evelop 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. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

Id. § 14/15(a).

28. With respect to informed consent, BIPA provides that:

No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information, 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) 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.

Id. § 14/15(b).

29. BIPA provides for statutory damages, injunctive relief, reasonable attorney’s fees and costs, and other relief “as the State or federal court may deem appropriate” when a private entity violates a consumer’s rights under the statute. *Id.* § 14/20. Where a violation is the result of a private entity’s negligence, BIPA provides for the greater of actual damages or \$1,000 in liquidated damages per violation, and, if the violation was intentional or reckless, BIPA provides for the greater of actual damages and liquidated damages of \$5,000 per violation. *Id.*

B. Defendants Collect Their Customers’ Biometric Identifiers and Information Through Voice ID

30. Verizon boasts that it “is one of the world’s leading providers of communications, technology, information and entertainment products and services to consumers, businesses and government entities” that “offer[s] data, video and voice services and solutions on our networks and platforms that are designed to meet customers’ demand for mobility, reliable network connectivity and security.”¹

31. Relevant here, Verizon’s Consumer Group provides cellular services and equipment to its retail customers in Illinois and across the United States, doing so “under the Verizon family of brands.”² While it does not publicly break down its customer base by state, Verizon reported that as of December 31, 2023, it had approximately 115 million wireless retail customers—over

¹ 2023 Form 10-K at 4.

² *Id.*

34% of the U.S. population.³ The Consumer Group is one of two of Verizon’s reportable segments and is extremely lucrative. In 2023, the Consumer Group’s revenues were \$101.6 billion, which represented approximately 76% of Verizon’s consolidated revenues.⁴

32. Beginning in 2021, Defendants began offering a service called Voice ID. Defendants maintain a webpage with a series of frequently asked questions (“FAQs”) relating to Voice ID, at <https://www.verizon.com/support/voice-id-faqs/> (the “Voice ID FAQs”). This undated webpage, however, does not purport to be any sort of BIPA-compliant Voice ID or biometric policy, and Defendants do not hold it out as such. In fact, Defendants maintain purported specific privacy policies for residents of California, Colorado, Connecticut, Main, Nevada, Oregon, Texas, Utah, Virginia, and Washington.⁵

State Privacy Rights

Some state laws provide additional privacy rights to residents.

[California](#)

[Colorado](#)

[Connecticut](#)

[Maine](#)

[Nevada](#)

[Oregon](#)

[Texas](#)

[Utah](#)

[Virginia](#)

[Nevada and Washington Health Privacy Notice](#)

There is no justification for Defendants’ failure to maintain any privacy policy specific to Illinois, Illinois residents, or BIPA. To the contrary, the omission is reckless, if not intentional.

³ *Id.*

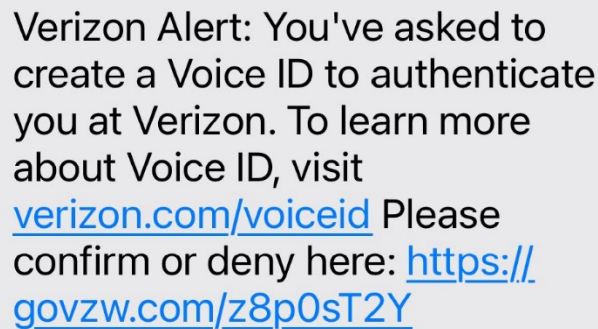
⁴ *Id.*

⁵ <https://www.verizon.com/about/privacy/> (last visited September 5, 2024).

33. On the FAQ page, Defendants describe Voice ID as “our biometrics system that uses your voice, with your consent, to help authenticate your account when you call Verizon.”⁶ Voice ID is not limited to Verizon Wireless cellular phone customers. Rather, Verizon also offers Voice ID to Fios Home Internet, Fios TV, or Fios Digital Voice customers.⁷

34. Defendants explain that “we only enroll you with your consent,” that “[o]nce enrolled, we’ll send you a notification by email, text, mail or voice call when your Voice ID is created,” and that “you can still remove Voice ID and delete your voiceprint, anytime.”⁸ This “consent,” however, is illusory and not remotely valid under BIPA.

35. When a customer enrolls in Voice ID (or is asked by one of Defendants’ customer service representatives to enroll in Voice ID), that customer receives the following text message:

A screenshot of a text message from Verizon. The text reads: "Verizon Alert: You've asked to create a Voice ID to authenticate you at Verizon. To learn more about Voice ID, visit [verizon.com/voiceid](https://www.verizon.com/voiceid) Please confirm or deny here: <https://govzw.com/z8p0sT2Y>". The text is displayed in a light gray speech bubble with a white background.

Verizon Alert: You've asked to create a Voice ID to authenticate you at Verizon. To learn more about Voice ID, visit [verizon.com/voiceid](https://www.verizon.com/voiceid) Please confirm or deny here: <https://govzw.com/z8p0sT2Y>

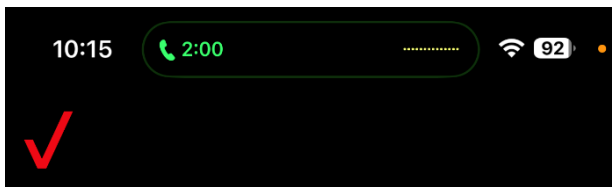
36. The customer is also directed to the following page in their browser to complete the enrollment process:⁹

⁶ <https://www.verizon.com/support/voice-id-faqs/> (last visited September 5, 2024).

⁷ *Id.*

⁸ *Id.*

⁹ All screenshots herein are accurate as of the date of the filing of this Complaint.



Consent to enroll in Voice ID

You've asked to enroll in Voice ID to use to authenticate you at Verizon. To learn more about Voice ID, visit: verizon.com/voiceid. Verizon will never call you to approve this request.

Date & Time

Tuesday, April 16, 2024
10:15 AM EDT

Verizon will never call you to approve this request.

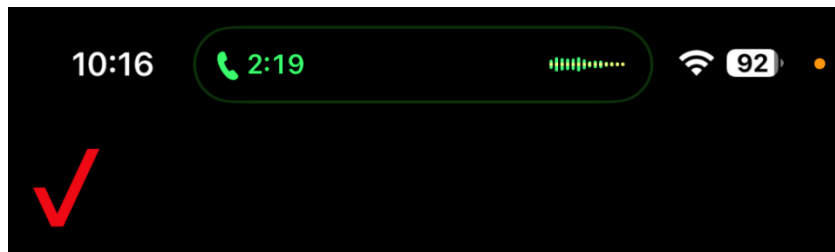
Do you want to grant consent to enroll in Voice ID?

- Enroll in Voice ID**
- Deny Request**

Submit

37. To enroll, a customer chooses the “Enroll in Voice ID” option and clicks “Submit.”

The customer is then presented with the following page in their browser:



Voice ID consent granted

You have consented to enroll in Voice ID. To learn more about Voice ID, visit: [verizon.com/voiceid](https://www.verizon.com/voiceid).

You can close out of this page and return to the original page to continue.

38. To finish the enrollment process, the customer is required to repeat a passphrase. Through the Voice ID enrollment process, Defendants collect a customer's voiceprint, which is a unique biometric identifier and/or biometric information under BIPA.

39. If clicked on, the hyperlinks shown in ¶¶35-37 above, [verizon.com/voiceid](https://www.verizon.com/voiceid), automatically redirect to the Voice ID FAQs, at <https://www.verizon.com/support/voice-id-faqs/>. While the communications in ¶¶35-37 include a link to the Voice ID FAQs, the Voice ID FAQs themselves are not, and Defendants do not purport them to be, a "written policy" within the meaning of BIPA. Critically, Defendants do not require a customer to review or consent to the Voice ID FAQs before enrolling in Voice ID.

40. At no point during the enrollment process were customers informed in writing that a biometric identifier and/or biometric information were being collected or stored. While the communications in ¶¶35-37 refer to "create[ing] a Voice ID" and "enroll[ing] in Voice ID," none of those communications state that a customer's *voiceprint*, i.e., a biometric identifier, is being collected or stored. Similarly, none of those communications state that by creating a Voice ID or

enrolling in Voice ID, Defendants would be collecting or storing that customers' voiceprint, which is a biometric identifier and/or biometric information.

41. At no point during the enrollment process were customers informed in writing of the specific purpose and length of term for which a biometric identifier or biometric information was being stored. Indeed, the communications in paragraphs ¶¶35-37 are entirely silent with respect to any time periods at all. And while the communication in ¶36 states that "Voice ID" would be used "to authenticate you" (which does not appear at all in ¶35 or ¶37) that communication does not state that a customer's *biometric identifiers or biometric information* would be used to authenticate them. Moreover, this communication contradicts the Voice ID FAQs (which again are not a policy and not required to be reviewed prior to or during the Voice ID enrollment process), which state that "Voice ID" could have up to five different uses—with more in the future—including such amorphous and unexplained uses like "[h]elping us improve and personalize your services."¹⁰

42. At no point during the enrollment process did Defendants require a customer to execute and send to them a written release, based on informed consent.

43. Upon enrolling in Voice ID, a customer receives the following confirmatory email:

¹⁰ <https://www.verizon.com/support/voice-id-faqs/> (last visited September 5, 2024).

verizon Shop Support My Verizon


You're now enrolled in Voice ID.

Hi [REDACTED]

On April 16, 2024, a change was made to your account. You've been enrolled in Voice ID (voice recognition authentication). If you didn't request this change, please call 800-922-0204.

View FAQs for more information.

[View FAQs](#)



[Manage preferences](#) > [Shop accessories](#) >



[Phones](#) [Tablets](#) [Accessories](#) [Plans](#) [Verizon Up](#) [Stores](#) [My Verizon App](#)

 Account number ending in: [REDACTED]

© 2024 Verizon

This email was sent to [REDACTED]. We respect your privacy. Please review our [Privacy Policy](#). If you think this email was sent in error or you'd like to update your contact information, please visit our [preference center](#).

Verizon, One Verizon Way, Mail Code: 180WVB, Basking Ridge, NJ 07920

44. Additionally, the customer also receives the following text message confirming that they have enrolled in Voice ID:

Verizon Msg: You've enrolled in Voice ID (voice recognition authentication). If you didn't request this change, please call [800-922-0204](tel:800-922-0204)

45. After enrolling, Defendants use Voice ID each time a customer calls to authenticate that customer's account. To use Voice ID, customers either say the passphrase "[a]t Verizon my voice is my password" or let Voice ID operate in the background to identify them as they are speaking.¹¹ Thus, after enrolling in Voice ID, Defendants collect, capture, or otherwise obtain a customer's voiceprint every time that customer calls, so that they can compare it to the voiceprint they already have stored as a result of the enrollment process.

46. During subsequent calls while Voice ID was activated and used, customers were not informed in writing that a biometric identifier and/or biometric information were being collected or stored. Likewise, during subsequent calls while Voice ID was activated and used, customers were not informed in writing of the specific purpose and length of term for which their biometric identifiers and/or information were being stored. Finally, during subsequent calls while Voice ID was activated and used, Defendants did not require a customer to execute and send to them a written release, based on informed consent.

47. Defendants' failure to comply with BIPA's requirement of informed, written consent is particularly egregious given their history of failing to protect personally identifiable information. For example, in July of 2024 a wholly-owned subsidiary of Defendant Verizon Communications paid a \$16 million fine to the FCC for, among other violations, a data breach where threat actors had access to customers' personally identifiable information for nearly a year before the breach was discovered.

48. Similarly, in February of 2024, Defendant Verizon Communications reported an internal data breach exposing the personally identifiable information of nearly 63,000 employees.

¹¹ *Id.*

49. These incidents followed another data breach in October of 2022, when Verizon reported that an unauthorized third party had accessed pre-paid customer accounts and used their exposed partial credit card information to conduct SIM-swapping attacks.

C. Defendants Violated Plaintiffs' Rights Under BIPA

1. Mr. Parker

50. Mr. Parker has been a customer of Defendants for approximately 2-1/2 years. About two months after being a customer of Verizon, and while in Illinois, Mr. Parker, enrolled in Voice ID.

51. On multiple occasions while Voice ID was active on his account and while in Illinois, Mr. Parker called Defendants. Upon information and belief, Voice ID was used during each of these calls.

52. During the enrollment process and during subsequent calls to Defendants when Voice ID was activated and used, Mr. Parker was not informed that Defendants would be collecting his biometric identifiers or biometric information.

53. Nor during the enrollment process or during subsequent calls to Defendants when Voice ID was activated and used did Defendants ever inform Mr. Parker about the specific purpose for which his biometric identifiers and/or biometric information were being collected or stored, the length of term that his biometric identifiers or biometric information would be stored, when or whether they would be destroyed, or whether they would transfer his biometric information to a third party for processing.

54. During the enrollment process and during subsequent calls to Defendants when Voice ID was activated and used, Defendants never obtained, or attempted to obtain, Mr. Parker's informed, written consent to collect, capture, or otherwise obtain his biometric identifiers or biometric information. Mr. Parker never provided a written release to Defendants authorizing them

to collect, store, or use his voiceprint, which uniquely identifies him, either during the enrollment process or during subsequent calls to Defendants when Voice ID was activated and used.

55. Mr. Parker was not provided with a privacy policy either during the enrollment process or during subsequent calls to Defendants when Voice ID was activated and used. Further, Defendants did not make such policies readily accessible so that Mr. Parker could review them prior to enrolling in Voice ID or during subsequent calls to Defendants when Voice ID was activated and used.

2. Mr. Doyle

56. Mr. Doyle has been a customer of Defendants since 2019 and, while in Illinois, enrolled in Voice ID.

57. On multiple occasions while Voice ID was active on his account and while in Illinois, Mr. Doyle called Defendants. Upon information and belief, Voice ID was used during each of these calls.

58. During the enrollment process and during subsequent calls to Defendants when Voice ID was activated and used, Mr. Doyle was not informed that Defendants would be collecting his biometric identifiers or biometric information.

59. Nor during the enrollment process or during subsequent calls to Defendants when Voice ID was activated and used did Defendants ever inform Mr. Doyle about the specific purpose for which his biometric identifiers and/or biometric information were being collected or stored, the length of term that his biometric identifiers or biometric information would be stored, when or whether they would be destroyed, or whether they would transfer his biometric information to a third party for processing.

60. During the enrollment process and during subsequent calls to Defendants when Voice ID was activated and used, Defendants never obtained, or attempted to obtain, Mr. Doyle's

informed, written consent to collect, capture, or otherwise obtain his biometric identifiers or biometric information. Mr. Doyle never provided a written release to Defendants authorizing them to collect, store, or use his voiceprint, which uniquely identifies him, either during the enrollment process or during subsequent calls to Defendants when Voice ID was activated and used.

61. Mr. Doyle was not provided with a privacy policy either during the enrollment process or during subsequent calls to Defendants when Voice ID was activated and used. Further, Defendants did not make such policies readily accessible so that Mr. Doyle could review them prior to enrolling in Voice ID or during subsequent calls to Defendants when Voice ID was activated and used.

V. CLASS ACTION ALLEGATIONS

62. Plaintiffs bring this action as a class action pursuant to Rules 23(a), 23(b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of a class defined as:

All persons whose biometric identifiers or biometric information was captured by Defendants through the use of Voice ID while residing (and/or present) in Illinois from September 13, 2019 to the present.

63. Excluded from the Class are: (a) Defendants and any of their members, affiliates, parents, subsidiaries, officers, directors, employees, successors, or assigns; (b) class counsel and their employees; and (c) the judicial officers and Court staff assigned to this case and their immediate family members.

64. This action has been brought and may properly be maintained on behalf of the Class proposed herein under the prerequisites of Rule 23 of the Federal Rules of Civil Procedure.

65. Ascertainability: The Class can be readily identified through Defendants' records. By filtering Defendants' customer database to records of Illinois residents who enrolled in Voice ID over the past five years and called Defendants while Voice ID was active on their accounts, and removing any excluded individuals from that list, the Class members may be readily identified.

66. Numerosity (Fed. R. Civ. P. 23(a)(1)): The Class is sufficiently numerous such that individual joinder of all Class members is impracticable. While Plaintiffs believe that there could be thousands or tens of thousands of Class members, the precise number of Class members is presently unknown to Plaintiffs, but may be ascertained from Defendants' records.

67. Commonality and Predominance (Fed. R. Civ. P. 23(a)(2)): This action involves common questions of law and fact, which predominate over any questions affecting only individual Class members, including, without limitation:

- a. Whether Verizon or Verizon Wireless qualify as a "private entity" as defined by BIPA, 740 ILCS 14/10;
- b. Whether Defendants capture, collect, store, or distribute information that qualifies as "biometric identifiers" or "biometric information" from Voice ID users, as defined by BIPA, 740 ILCS 14/10 & 14/15, *et seq.*;
- c. Whether Defendants obtained an executed written release from each user of Voice ID before capturing their biometric identifiers and/or biometric information as required by BIPA, 740 ILCS 14/15(b);
- d. Whether Defendants previously, or on an ongoing basis, collected, captured, purchased, received through trade, or otherwise obtained the biometric identifiers and/or biometric information of Voice ID users, in violation of BIPA, 740 ILCS 14, *et seq.*;
- e. Whether Defendants' conduct was and is willful, reckless, or negligent;
- f. The appropriate measure of damages to award Plaintiffs and the other Class members; and
- g. The appropriate injunctive relief to which Plaintiffs and the other Class members are entitled.

68. Typicality (Fed. R. Civ. P. 23(a)(3)): Plaintiffs' claims are typical of the other Class members' claims because Plaintiffs and each of the other Class members were users of Voice ID, through which Defendants collected, captured, purchased, received through trade, or otherwise obtained their biometric identifiers and/or biometric information. Defendants did not inform Plaintiffs or the other Class members of such collection, capture, purchase, receiving through trade,

or otherwise obtaining of such biometric identifiers and/or biometric information, and did not obtain written consent for this same capture, collection, purchase, receiving through trade, or otherwise obtaining of biometric identifiers and/or biometric information from Plaintiffs or the other Class members.

69. Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)): Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members whom they seek to represent. Plaintiffs intend to vigorously prosecute this action, and Class members' interests will be fairly and adequately protected by Plaintiffs and their chosen counsel. Plaintiffs have retained counsel that is competent and experienced in complex class action and other privacy litigation (including successfully litigating class action cases similar to this one, where a defendant breached statutory privacy obligations), and Plaintiffs' counsel will devote the time and financial resources necessary to vigorously prosecute this action. Neither Plaintiffs nor their counsel have any interests adverse to the Class.

70. Declaratory and Injunctive Relief (Fed. R. Civ. P. 23(b)(2)): Defendants acted or refused to act on grounds generally applicable to Plaintiffs and the other Class members, such that final injunctive and declaratory relief is appropriate with respect to the Class as a whole.

71. Superiority (Fed. R. Civ. P. 23(b)(3)): A class action is superior to individual adjudications because joinder of all class members is impracticable, would create a risk of inconsistent or varying adjudications, and would impose an enormous burden on the judicial system. The amount-in-controversy for each individual class member is likely relatively small, which reinforces the superiority of representative litigation. As such, a class action presents far fewer management difficulties than individual adjudications, preserves the resources of the parties and the judiciary, and protects the rights of each class member.

VI. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION

Violation of BIPA, 740 ILCS 14/15(b)

Against all Defendants

(Failure to inform in writing and obtain written releases from customers prior to capturing, collecting, or storing biometric identifiers and/or biometric information)

72. Plaintiffs reassert, reallege, and incorporate by reference paragraphs 1 to 71.

73. Plaintiffs bring this claim individually and on behalf of all other Class Members.

74. Defendants' Voice ID captured, and continues to capture, Plaintiffs' and the other Class members' biometric identifiers and/or biometric information, including their voiceprints, both during the enrollment process and during subsequent calls when Voice ID was activated and used.

75. Voiceprints are a biometric identifier protected by BIPA.

76. On information and belief, when they collected Plaintiffs' and Class Members' voiceprints, Defendants also collected, captured or otherwise obtained biometric information based on Plaintiffs' and Class Members' voiceprints.

77. BIPA prohibits private entities like Verizon and Verizon Wireless from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining customers' biometric identifiers or biometric information without first informing them in writing of such activities; informing them in writing of the specific purpose and length of term for which biometric identifiers or biometric information are being collected, stored, and used; and obtaining a written release based on informed consent executed by the customers whose biometric identifiers or biometric information is being collected.

78. During the Voice ID enrollment process and during subsequent calls when Voice ID was activated and used, Defendants did not inform Plaintiffs and Class Members in writing that their customers' biometric identifiers and/or biometric information will be collected; did not

inform Plaintiffs and Class Members in writing of the specific purpose and length of time that their customers' biometric identifiers and/or biometric information will be collected, stored, and used; and did not obtain written consent from Plaintiffs and Class Members based on informed consent affirming that, by using Voice ID, their biometric identifiers and/or biometric information will be collected.

79. Upon information and belief, Defendants are continuing to collect, capture, and store biometric identifiers and/or biometric information of Voice ID users, without the specific informed consent required by BIPA.

80. Defendants' violations of BIPA section 15(b) were either intentional or reckless, or, pleaded in the alternative, negligent.

81. Plaintiffs and the other Class members have been injured by Defendants' conduct alleged herein, which injury includes the unknowing loss of control of their most unique biometric identifiers and/or biometric information, and violations of their privacy due to Defendants' collection, capture, and storage of their biometric identifiers and/or biometric information. Accordingly, Plaintiffs seek: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Classes by requiring Defendants to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and/or biometric information as described herein; (2) statutory damages of \$5,000 for each willful and/or reckless violation of the BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of \$1,000 for each negligent violation of the BIPA pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees, costs, and expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION

Violation of BIPA, 740 ILCS 14/15(e)

Against all Defendants

(Failure to protect customers' biometric identifiers and/or biometric information from disclosure)

82. Plaintiffs reassert, reallege, and incorporate by reference paragraphs 1 to 71.

83. Plaintiffs bring this claim individually and on behalf of all other Class members.

84. As alleged above, Defendants have an extensive history of failing to protect personally identifiable information.

85. Upon information and belief, Defendants violated BIPA when they failed to adequately protect Plaintiffs and Class members' biometrics from disclosure in accordance with the reasonable standard of care within their industry or in a manner that is the same as or more protective than the manner in which Defendants protect other confidential and sensitive information.

86. Defendants' violations of BIPA section 15(e) alleged herein were either intentional or reckless, or, pleaded in the alternative, negligent.

87. Plaintiffs and the other Class members have been injured by Defendants' conduct, which injury includes the potential disclosure of their most unique biometrics to malign actors, and violations of their privacy due to Defendants' failure to adequately protect their biometrics. Accordingly, Plaintiffs seek: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Classes by requiring Defendants to comply with BIPA's requirements for the protection from disclosure of their biometrics as described herein; (2) statutory damages of \$5,000 for each willful and/or reckless violation of the BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of \$1,000 for each negligent violation of the BIPA pursuant to 740 ILCS 14/20(1); and (3) reasonable attorneys' fees, costs, and expenses pursuant to 740 ILCS 14/20(3).

VII. PRAYER FOR RELIEF

88. Plaintiffs, individually and on behalf of all others similarly situated, respectfully request the following relief:

- a. Finding that this action satisfies the requirements for maintenance as a class action as set forth in Rule 23 of the Federal Rules of Civil Procedure and certifying the Class defined herein;
- b. Appointing Plaintiffs as representatives of the Class and their undersigned counsel as class counsel;
- c. Entering judgment in favor of Plaintiffs and the other Class members and against Defendants;
- d. Awarding Plaintiffs and the other Class members liquidated damages of \$1,000 per negligent violation, \$5,000 per willful or reckless violation, or actual damages, whichever is greater, for each of Defendants' BIPA violations;
- e. Issuing an injunction ordering Defendants to comply with BIPA and enjoining them from engaging in further misconduct in violation of BIPA;
- f. Awarding reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses, as provided for in 740 ILCS 14/20; and
- g. Granting such other and further relief as the Court deems appropriate.

VIII. JURY TRIAL REQUESTED

89. Plaintiffs, individually and on behalf of all other Class members, request a trial by jury on all claims so triable.

Dated: September 13, 2024

Respectfully submitted,

/s/ Thomas M. Hanson

Jon Loevy
Michael Kanovitz
Thomas M. Hanson
Loevy & Loevy
311 North Aberdeen, 3rd Floor
Chicago, Illinois, 60607
(312) 243-5900
jon@loevy.com
mike@loevy.com
hanson@loevy.com

-and-

Brian Levin*
brian@levinlawpa.com
Brandon T. Grzandziel*
brandon@levinlawpa.com
LEVIN LAW, P.A.
2665 South Bayshore Drive, PH2
Miami, FL 33133
Telephone: (305) 402-9050
Facsimile: (305) 676-4443

-and-

Jeffrey B. Kaplan
jkaplan@dkrpa.com
Alexander M. Peraza
aperaza@dkrpa.com

**DIMOND KAPLAN & ROTHSTEIN,
P.A.**

2665 South Bayshore Drive, PH-2B
Miami, FL 33133
Telephone: (305) 374-1920
Facsimile: (305) 374-1961

Counsel for Plaintiffs and the Proposed Class

* *Pro Hac Vice* Admission Applications
Forthcoming