UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

CHRISTINE MCGOVERAN, JOSEPH VALENTINE, and AMELIA RODRIGUEZ, on behalf of themselves and all other persons similarly situated, known and unknown,	)	Case No.:
Plaintiffs,	)	**JURY TRIAL DEMANDED**
v.	)	**CLASS ACTION**
AMAZON WEB SERVICES, INC. and PINDROP SECURITY, INC.,	)	
Defendants.	)	

COMPLAINT

Plaintiffs Christine McGoveran, Joseph Valentine, and Amelia Rodriguez, ("Plaintiffs"), individually and on behalf of all other persons similarly situated, bring this class action lawsuit for violations of the Biometric Information Privacy Act, 740 ILCS 14/1 *et seq*. ("BIPA"), against Defendants Amazon Web Services, Inc. and Pindrop Security, Inc. Plaintiffs allege the following facts based upon personal knowledge, investigation by retained counsel, and on information and belief.

I. Nature of the Action

1. Plaintiffs allege that Defendants Pindrop Security, Inc. and Amazon Web Services, Inc. ("Defendants") violated BIPA by collecting, possessing, redisclosing, profiting from, and failing to safeguard their biometric identifiers and biometric information ("Biometric Data"). For the reasons discussed in greater detail below, Defendants' violations of BIPA pose a serious threat of permanent harm to Plaintiffs and members of the putative class.

2. Plaintiffs seek to represent a class of individuals who made one or more phone calls to or received one or more phone calls from call centers, customer service representatives and/or other entities using services offered by Amazon Web Services, Inc., and had their unique, biometric voiceprints collected, possessed, and used by Defendants without their consent or authorization, including through the use of Pindrop's biometric voice authentication technology.

3. Plaintiffs have suffered significant damage, as more fully described herein, because their Biometric Data has been intercepted, collected, and disseminated without their knowledge or consent, thereby 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.

4. Through this lawsuit, Plaintiffs, on behalf of a similarly situated class, seek to enjoin Defendants from collecting, possessing, and profiting from their Biometric Data in violation of BIPA, and seek to obtain actual and statutory damages for their injuries.

5. The remedies Plaintiffs seek are remedial, and not penal, in nature.

II. Parties

6. Plaintiff Christine McGoveran is a resident of Wood River in Madison County, Illinois.

7. Plaintiff Joseph Valentine is a resident of Antioch in Lake County, Illinois.

8. Plaintiff Amelia Rodriguez is a resident of Chicago in Cook County, Illinois.

9. Plaintiffs made phone calls to call centers using services provided by Defendant Amazon Web Services ("AWS") and had their biometric identifiers and biometric information collected, stored, and/or used by Defendants, as more fully described herein.

10. Defendant AWS is a Delaware corporation that is registered to and does conduct business throughout Illinois. AWS may be served with process through its registered agent, the Corporation Services Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

11. AWS is a "private entity" under the meaning of BIPA. *See* 740 ILCS 14/10.

12. Defendant Pindrop Security, Inc. ("Pindrop") is a Delaware corporation that is registered to and does conduct business throughout Illinois. Pindrop may be served with process through its registered agent, the Corporation Services Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

13. Pindrop is a "private entity" under the meaning of BIPA. *See* 740 ILCS 14/10.

III. Jurisdiction and Venue

14. This Court has general personal jurisdiction over Defendants because they are both Delaware corporations.

15. This Court has diversity subject matter jurisdiction over Defendants because the amount in controversy exceeds $75,000 and the dispute is between citizens of different States. 28 U.S.C. §1332 (a)(1). This Court also has subject matter jurisdiction under 28 U.S.C. §1332 (d)(2)(A) because this is a civil class action in which the amount in controversy exceeds $5,000,000, and at least one Class Member is a citizen of a State different from at least one Defendant.

16. Venue is proper pursuant to 28 U.S.C. § 1391(b)(1).

IV. The Biometric Information Privacy Act

17. "Biometrics" refers to "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.

18. BIPA was enacted in 2008 in order to safeguard biometric information 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.

19. As set forth in BIPA, biologically unique identifiers, such as voiceprint information, cannot be changed. 740 ILCS 14/5(c). As is likewise set forth in BIPA, the inalterable nature of biologically unique identifiers presents a heightened risk when biometric information is not protected in a secure and transparent fashion. 740 ILCS 14/5(d)–(g).

20. As a result of the need for enhanced protection of biometric information, BIPA imposes various requirements on private entities that collect or maintain individuals' biometric information, including voiceprints.

21. 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).

22. BIPA applies to entities that interact with two forms of Biometric Data: biometric "identifiers" and biometric "information." 740 ILCS 14/15(a)-(e).

23. "Biometric identifiers" are physiological, as opposed to behavioral, characteristics. Examples include, but are not limited to, voiceprints, face geometry, fingerprints, DNA, palmprints, hand geometry, iris patterns, and retina patterns. As the Illinois General Assembly has explained:

> Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric facilitated transactions.

740 ILCS 14/5(c). Moreover,

> A person cannot obtain new DNA or new fingerprints or new eyeballs for iris recognition, at least not easily or not at this time. Replacing a biometric identifier is not like replacing a lost key or a misplaced identification card or a stolen access code. The Act's goal is to prevent irretrievable harm from happening and to put in place a process and rules to reassure an otherwise skittish public.

Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, ¶ 59, 115 N.E.3d 1080, 1093, appeal denied, 119 N.E.3d 1034 (Ill. 2019). A "biometric identifier" is defined by BIPA as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

24. 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. In this case, the biometric identifiers at issue are the voiceprints of individuals, including Plaintiffs, intercepted by Defendants without any notice to or consent from the individuals whose biometric identifiers are collected.

25. "Biometric information" consists of biometric identifiers used to identify a specific person. "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.

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

(1) collecting Biometric Data, 740 ILCS 14/15(b);

(2) possessing Biometric Data, 740 ILCS 14/15(a);

(3) profiting from Biometric Data, 740 ILCS 14/15(c); and

(4) disclosing Biometric Data, 740 ILCS 14/15(d).

BIPA also created a heightened standard of care for the protection of Biometric Data. 740 ILCS 14/15(e).

27. 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 Biometric Data Under Section 15(b).

28. BIPA imposes three requirements that must be satisfied before any private entity may "collect, capture . . . or otherwise obtain" biometric information:

(a) First, the private entity must inform the individual in writing that the individual's biometric information is 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 biometric information is 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).

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

B. Possessing Biometric Data Under Section 15(a).

30. BIPA requires that any private entity in possession of biometric data develop a public, written policy "establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information." 740 ILCS 14/15(a).

31. BIPA requires that this public, written policy include information about how the entity will destroy the biometric data upon fulfilling the purpose for its collection or within three years, whichever is later. *Id*.

32. BIPA requires a private entity in possession of biometric data to "comply with its established retention schedule and destruction guidelines," that is, to actually destroy biometric data pursuant to its policies. *Id*.

C. BIPA's Unqualified Prohibition on Profiting from Biometric Data Under Section 15(c).

33. BIPA additionally bars private entities from profiting from Biometric Data. 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).

34. Section 15(c) is an unqualified prohibition on profiting from Biometric Data. Section 15(c) applies to this case, for among other reasons, because Defendants developed, sold, operated, and profited from Plaintiffs' Biometric Data.

35. BIPA forbids any private entity in possession of a biometric identifier or biometric information from "profit[ing]" from that data. 740 ILCS 14/15(c).

D. Disseminating Biometric Data Under Section 15(d).

36. BIPA prohibits the "disclos[ure], redisclos[ure], or other[] disseminat[ion]" of biometric data 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).

E. Standard of Care for Biometric Data Under Section 15(e).

37. BIPA requires that any private entity in possession of biometric data "store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry[.]" 740 ILCS 14/15(e)(1).

38. In addition, BIPA requires that any private entity in possession of biometric data "store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information." 740 ILCS 14/15(e)(2).

V. The Serious Threats Posed by Biometric Data

39. Voice biometrics—also known as voiceprinting—uses biological characteristics to verify an individual's identify.

40. For example, voice biometrics may be used to confirm the identity of a caller to a customer service agent or a call center.

41. Operators of call centers and/or customer service operations may, for various reasons, desire to avoid authenticating callers using traditional methods, such as the use of a passcode or answers to secret questions, and instead choose to authenticate callers using voice biometrics, including voiceprints.

42. When a passcode is used as a security measure, in the event of a data breach an individual may simply change the passcode to prevent unauthorized access to the individual's compromised account. By contrast, when call centers or customer service personnel use voice biometrics for authentication, in the event of a data breach there is nothing an individual can do to prevent someone from using the individual's voice biometrics to gain unauthorized access to the compromised account.

43. The global voice biometrics market size is expected to grow dramatically—according to one source, from $984 million in 2019 to $2.8 billion by 2024.[1]

44. "Stolen biometric identifiers . . . can be used to impersonate consumers, gaining access to personal information."[2]

45. Unlike other identifiers such as Social Security or credit card numbers, which can be changed if compromised or stolen, biometric identifiers linked to a specific voice or face cannot be modified—ever. These unique and permanent biometric identifiers, once exposed, leave victims with no means to prevent identity theft and unauthorized tracking.

46. Once a person or entity has an individual's Biometric Data:

> [T]hey can get your name, they can find your social networking account, and they can find and track you in the street, in the stores that you visit, the . . . buildings you enter, and the photos your friends post online.[3]

---

[1] *Voice Biometrics Market Worth $2,845 Million by 2024*, Cision PR Newswire (May 2, 2019), https://www.prnewswire.com/news-releases/voice-biometrics-market-worth-2-845-million-by-2024---exclusive-report-by-marketsandmarkets-300842635.html, *archived at* https://perma.cc/8WYU-KW9A.

[2] Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 629 (2019).

[3] *What Facial Recognition Technology Means for Privacy and Civil Liberties*, Hearing Before the Subcomm. On Privacy Tech & the Law of the S. Comm. On the Judiciary, 112th Cong. 1 (Jul. 18, 2012), at 1, 2, https://www.congress.gov/112/chrg/CHRG-112shrg86599/CHRG-112shrg86599.pdf, *archived at* https://perma.cc/2F9Y-S8HQ (statement of

47. Indeed, the Illinois Supreme Court has held that in BIPA the Illinois "General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach*, 129 N.E.3d at 1206.

48. In so holding, the Court explicitly recognized the "difficulty in providing meaningful recourse once a person's biometric identifiers or biometric information has been compromised." *Id*. As it further held, "[t]he situation is particularly concerning, in the legislature's judgment, because [t]he full ramifications of biometric technology are not fully known.'" *Id*. (citing BIPA).

49. The use of Biometric Data "leads to the fear that a data breach or sale by one holder of a piece of a person's biometric information would compromise the security of all relationships that are verified by that same piece."[4]

50. This fear is not based on mere conjecture. Biometric Data has been illicitly targeted by hackers. For example, a security firm recently uncovered a "major breach" of a biometric system used by banks, police, defense firms, and other entities.[5] This breach involved exposure of extensive biometric and other personal data, including facial recognition data and fingerprints. *Id*.

Sen. Al Franken, raising concerns about the implications of the rising use of facial racial recognition technology to the Subcommittee on Privacy, Technology, and the Law).

[4] Matthew B. Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 UC Irvine L. Rev. 107, 132 (2019).

[5] Josh Taylor, *Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms*, The Guardian (Aug. 14, 2019), https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms, *archived at* https://perma.cc/A848-6JMM (reporting that the "fingerprints of over 1 million people, as well as facial recognition information…was discovered on a publicly accessible database").

51. Even anonymized Biometric Data poses risks. For example, according to a recent report:

> In August 2016, the Australian government released an "anonymized" data set comprising the medical billing records, including every prescription and surgery, of 2.9 million people. Names and other identifying features were removed from the records in an effort to protect individuals' privacy, but a research team from the University of Melbourne soon discovered that it was simple to re-identify people, and learn about their entire medical history without their consent, by comparing the dataset to other publicly available information, such as reports of celebrities having babies or athletes having surgeries.[6]

Indeed, "[t]here is a growing skepticism in the field of data protection and privacy law that biometric data can never truly be deidentified or anonymized."[7]

VI. Defendants Violated BIPA and Exposed Plaintiffs to Serious Harms

A. Defendants' Collection, Possession, and Use of Biometric Data.

52. Pindrop offers voice biometric services.

53. Pindrop's voiceprint services are used by call centers and customer service personnel to confirm the identity of individual callers.

54. Pindrop advertises products and services that confirm the identity of the speaker by voice.[8]

---

[6] Olivia Solon, *'Data Is A Fingerprint': Why You Aren't as Anonymous As You Think Online*, The Guardian (Jul. 13, 2018), https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy, *archived at* https://perma.cc/CD9K-GQ7T ("So-called 'anonymous' data can be easily used to identify everything from our medical records to purchase histories").

[7] Justin Banda, *Inherently Identifiable: Is It Possible To Anonymize Health And Genetic Data?*, International Association of Privacy Professionals Privacy Perspectives (Nov. 13, 2019), https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data/, *archived at* https://perma.cc/E5VZ-2YNJ.

[8] Pindrop website homepage, https://www.pindrop.com, *archived at* https://perma.cc/X5XJ-KGLR .

55. Pindrop describes its software as being able to "authenticate callers" by "extracting . . . intelligence from every call encountered."[9]

56. Pindrop's "Deep Voice" product uses "biometrics" to "identify[] and analyz[e]" repeat callers."[10]

57. Similarly, Pindrop's "Phoneprinting" product analyzes call audio to "create a distinctive identifier for each caller."[11]

58. Pindrop charges fees for and profits from the voiceprint products and services it offers, including those described herein.

59. AWS offers cloud storage services, offering its customers the ability to store their data, access their data remotely, and create backup copies of data.

60. AWS also offers call center services under the brand "Amazon Connect."

61. Amazon Connect is a "cloud-based contact center service."[12]

62. In connection with Amazon Connect, AWS possesses and stores a variety of types of customer data.

63. AWS obtains and stores biometric identifiers and biometric information for its customers.

---

[9] Amazon Connect Pindrop Integration Guide, https://aws.amazon.com/quickstart/connect/pindrop/, at 3, *archived at* https://perma.cc/3LJG-47KE ("Analytics for contact center security in the AWS Cloud").

[10] Deep Voice for Speaker Identification, https://www.pindrop.com/technologies/deep-voice/, *archived at* https://perma.cc/3XLG-S24Y.

[11] About Phoneprinting Technology, https://www.pindrop.com/resources/video/video/about-phoneprinting-technology/, *archived at*https://perma.cc/UK2R-25FN.

[12] Introducing Amazon Connect (Mar. 28, 2017), https://aws.amazon.com/about-aws/whats-new/2017/03/introducing-amazon-connect/, *archived at* https://perma.cc/ZJ2W-DUVM.

64. AWS advertises that Amazon Connect is capable of "integrat[ing] with a broad set of AWS tools and infrastructure[.]"[13]

65. AWS and Pindrop publicly advertise the availability of a Pindrop "integration with Amazon Connect[.]"[14]

66. Pindrop, in a November 27, 2017 press release, touted that it was "one of the first" partners with AWS in launching the "new Amazon Connect offering."[15] Further, Pindrop asserted that its integration with Amazon Connect was "native."[16]

67. Pindrop's voice authentication services are offered by AWS to Amazon Connect customers.

68. When integrated with an Amazon Connect implementation, Pindrop's voice authentication service uses biometric analysis of call audio to determine the identity of callers.

69. AWS charges fees for and profits from its Amazon Connect services.

70. AWS profits from offering Pindrop's voiceprint services in conjunction with its Amazon Connect services.

71. AWS advertises Pindrop integration as a selling point and added value for Amazon Connect customers.

---

[13] *Id.*

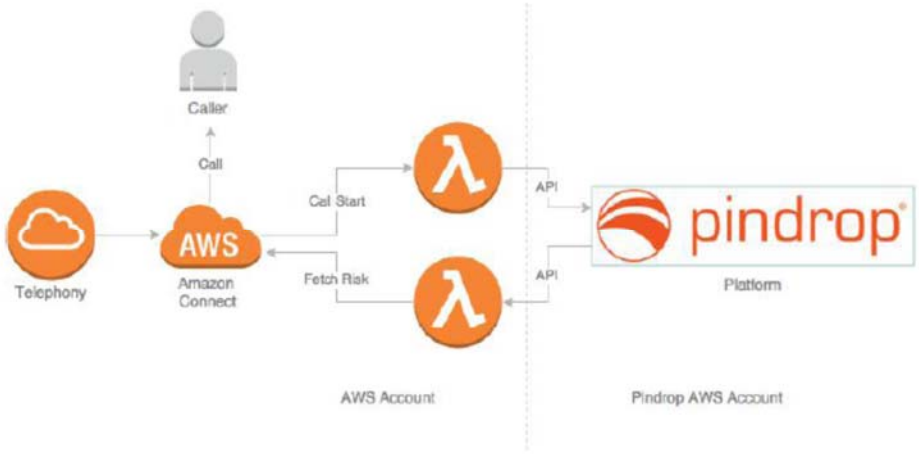
[14] Amazon Connect Pindrop Integration Guide, https://aws.amazon.com/quickstart/connect/pindrop/, at 1, *archived at* https://perma.cc/84JH-6U2W (This document while branded with Pindrop logos also is marked as "copyright © 2017 Amazon Web Services, Inc., and/or its affiliates").

[15] Amazon Connect Certifies Pinrop's Security and Authentication Technology (Nov. 27, 2017), https://www.businesswire.com/news/home/20171127005113/en/Amazon-Connect-Certifies-Pindrops-Security-Authentication-Technology, *archived at* https://perma.cc/4FR8-WEXX.

[16] *Id.*

72. AWS uses Pindrop integration to distinguish AWS's call center services from the call center services offered by AWS's competitors.

73. AWS and Pindrop describe this integration, among other ways, with the following diagram:



74. Pindrop describes the above figure as a "[d]ataflow diagram of Pindrop architecture within Amazon Connect."[17]

75. This diagram demonstrates that audio from incoming calls to call centers, such as those Plaintiffs contacted, is sent to Pindrop for processing. The output from that processing is returned to AWS's servers.[18]

76. Pindrop advertises that its services are "cloud-based." In other words, Pindrop hosts Plaintiffs' and the Class's biometric data on its servers. Pindrop exclusively controls these servers.

[17] Amazon Connect Pindrop Integration Guide, https://aws.amazon.com/quickstart/connect/pindrop/, at 1, *archived at* https://perma.cc/69F6-2FC3.

[18] *Id.*

77. Indeed, Pindrop stated on its website that its services "eliminate the need to purchase and deploy an extensive hardware infrastructure—allowing enterprises to avoid operational and capital expenditure historically tied to on-premises equipment[]."[19]

78. The analysis of intercepted telephone calls to extract biometric data takes place in part on Pindrop's servers, and is done via software developed, maintained, and controlled by Pindrop.

79. As the foregoing allegations make clear, the biometric data of Plaintiffs and the Class are stored on AWS's servers. Further, the private information of Plaintiffs and the Class stored on AWS's servers in connection with its Amazon Connect product is matched by AWS to biometric identifiers supplied by Pindrop, creating biometric information. After compiling this biometric information, AWS stores this biometric information on its servers.

80. When Pindrop's services are integrated with an Amazon Connect implementation, AWS collects and possesses "biometric information" as defined by BIPA.

81. AWS stores biometric templates on its servers as part of the arrangement alleged herein.

82. Defendants gathered data about Illinois callers including their phone numbers.

83. Part of the function of the AWS-Pindrop biometric data extraction system is to match callers, based on their voice biometrics, with other personally identifiable information, including location.

[19] Pindrop website, *Passive, Multi-Factor Authentication*, https://www.pindrop.com/solutions/authentication/, *archived at* https://perma.cc/WAG2-HBNF (asserting Pindrop's "passive, multi-factor authentication" helps contact centers authenticate "legitimate callers quickly and accurately" while reducing "call handle times").

84. Defendants, at all relevant times, knew that they were extracting biometric information from calls originating in Illinois, from Illinois citizens, using Illinois phone numbers.

85. Defendants knew that they were extracting this biometric data from call audio intercepted in Illinois.

86. However, Defendants fail to obtain informed written consent prior to collecting this biometric information as required by BIPA section 15 (b).

87. Further, Defendants have not made available to the public a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information, as required by BIPA section 15 (a).

88. Defendants have failed to destroy Plaintiffs' biometric data as is required by BIPA section 15(a).

89. As is evident from the facts alleged herein, AWS, Pindrop, and their corporate customers also "disclose, redisclose, and disseminate" to and between each other the biometric information and biometric identifiers of callers. *See* BIPA section 15(d).

90. However, Defendants do not obtain consent for this disclosure, redisclosure and dissemination, as required by BIPA section 15(d).

91. In addition, Defendants profit from the use of biometric data, in violation of BIPA section 15(c).

92. Finally, on information and belief, Defendants fail to apply the industry standard of care in storing, transmitting, and protecting from disclosure biometric data, and fail to apply a standard of care which is the same as or more protective than the manner in which they protect other confidential information, including, but not limited to healthcare data, in violation of BIPA section 15(e).

B. Defendants Collection and Possession of Plaintiffs' Biometric Data.

93. Plaintiffs called John Hancock customer service representatives and/or call center(s) on numerous occasions, from Illinois, using Illinois telephone numbers.

94. For example, Plaintiff Christine McGoveran has called John Hancock call center(s) and/or customer service representatives regarding her 401(k) account with John Hancock on several occasions, including twice in April and June of 2019.

95. Similarly, Plaintiff Joseph Valentine called John Hancock call center(s) and/or customer service representatives regarding his 401(k) account with John Hancock on multiple occasions.

96. Likewise, Plaintiff Amelia Rodriguez has called John Hancock call center(s) and/or customer service representatives regarding a John Hancock annuity on more than one dozen occasions in recent years, most recently in November 2019.

97. John Hancock's call center(s) use Amazon Connect with Pindrop biometric voiceprint authentication.

98. Because John Hancock's call center(s) use this technology, they "no longer require[] customers to have a pin for authentication." [20] Instead they use Pindrop's "voice biometrics" to authenticate callers.[21]

99. As is evident from the foregoing allegations, Plaintiff called John Hancock call centers that had implemented Defendants' biometric data collection technology.

[20] Salesforce website, *Why John Hancock Uses Salesforce & Amazon Connect for its Call Center*,https://www.salesforce.com/products/service-cloud/resources/john-hancock-contact-center/, *archived at* https://perma.cc/6PTX-CQHW.

[21] *Id.*

100. AWS and Pindrop apply their voice biometric technology to every caller to John Hancock's call center(s).

101. AWS knowingly intercepted the telephone calls made by Plaintiffs to John Hancock and collected and stored Plaintiffs' biometric data harvested from those calls.

102. Pindrop knowingly accepted and analyzed intercepted telephone calls to collect and store Plaintiffs' biometric data.

C. Defendants Profit from Plaintiffs' Biometric Data.

103. Defendants profit (i.e., "derive benefit")[22] from their collection and possession of Plaintiffs' biometric data.

104. Pindrop profits from Plaintiffs' Biometric Data by selling Pindrop's biometric data analysis and software as a service.[23] Pindrop receives and analyzes audio of Plaintiffs' voices, then disseminates the resulting sensitive Biometric Data to its customers, a service for which it is paid. Pindrop does not tell Plaintiffs it is profiting from its harvesting of their biological information, nor does it obtain their consent. Even if it did obtain consent—though it did not—Pindrop's practice of profiting from Plaintiffs' biometric data is a BIPA violation. BIPA section 15(c).

105. AWS profits from Plaintiffs' Biometric Data because, as alleged herein, it is paid to collect and store this data, which it knowingly does without Plaintiffs' knowledge or consent. Further, AWS advertises the availability of Amazon Connect's integration with Pindrop as a selling point to obtain customers, from whom it generates sales and profits.

[22] Merriam-Webster Dictionary, definition of *profit*, https://www.merriam-webster.com/dictionary/profit, *archived at* https://perma.cc/75X4-WDBT.

[23] Pindrop website homepage, https://www.pindrop.com, *archived at* https://perma.cc/X5XJ-KGLR.

106. In addition to physically hosting Plaintiffs' Biometric Data, AWS supports the Amazon Connect-Pindrop integration in an ongoing fashion to ensure that the AWS and Pindrop systems continue to work together to analyze Biometric Data. AWS uses this ongoing support as a selling point to attract customers.

107. Defendants used the features of their services described herein to compete with similar features being offered as part of other call center solutions, giving Defendants a competitive edge that allowed Defendants to profit from the sale of their services.

108. For the reasons set forth above, among others, Defendants profit from Biometric Data.

109. Defendants are prohibited from profiting from any "person's or . . . customer's biometric information" because Defendants are "private entit[ies] in possession of a biometric identifier." 740 ILCS 14/15(c). Therefore, the fact that Defendants profit from the Biometric Data they collect in Illinois is unlawful.

D. Defendants' Conduct Violates BIPA.

110. Plaintiffs' voice audio was intercepted in Illinois by Defendants.

111. Defendants performed biometric analysis to extract biometric data from audio taken from Illinois.

112. Though Defendants are aware that they are intercepting audio in Illinois and conducting biometric voice analysis on Illinois citizens, Defendants do not inform these Illinois callers that their biometric information and biometric identifiers are being collected and stored.

113. Defendants do not obtain consent from callers to these call centers, in any form, prior to collecting and storing their voiceprints, let alone obtain written, informed consent, as required by BIPA.

114. Further, contrary to the requirements of BIPA, neither AWS nor Pindrop have developed any written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information.

115. Defendants have collected, captured, obtained, and possessed the biometric information and biometric identifiers of Plaintiffs in violation of BIPA.

116. Defendants have profited from the use of Plaintiffs' biometric information, in violation of BIPA.

117. Pindrop, after collecting Plaintiffs' and the Class's biometric data, disclosed and disseminated that data to AWS.

118. AWS, after receiving from Pindrop and storing Plaintiffs' and the Class's biometric data, redisclosed and disseminated that data to AWS's Amazon Connect customers.

119. Defendants disseminated, between each other and their call center clients, the biometric data of Plaintiffs, regardless of whether such dissemination was required in order to complete a financial transaction or was required by law, in violation of BIPA.

120. Defendants also failed to use reasonable standards of care in storing, transmitting and protecting from disclosure Plaintiffs' biometric information and biometric identifiers, including by failing to treat Plaintiffs' biometric data with the same degree of care they applied to other confidential data, such as healthcare data.

121. As alleged herein, Defendants disclose and re-disseminate Plaintiffs' and Class members' biometric information for profit, and otherwise mishandle said biometric information.

122. Defendants fail to "store, transmit, and protect from disclosure" Plaintiffs' and Class Members' biometric identifiers and biometric in a manner that is the same as or more protective than the manner in which they store, transmit, and protect other confidential and

sensitive information. For example, upon information and belief, Defendants do not disclose and re-disseminate for profit their employees' healthcare records.[24]

VII. Class Allegations

123. Plaintiffs seek to represent the following class (the "Class") of similarly situated individuals:

> All Illinois citizens who placed one or more phone calls to, or received one or more phone calls from, an entity using Amazon Connect and Pindrop's voice authentication and/or fraud detection technology, from December 17, 2014 until present.

124. Numerosity. The Class includes thousands of people, such that it is not practicable to join all Class members into one lawsuit.

125. Ascertainability. The identity of Class members is ascertainable and identifiable based on Defendants' records.

126. Commonality. The issues involved with this lawsuit present common questions of law and fact, including:

- whether Defendants collected and/or possessed the Class's "biometric identifiers" or "biometric information";
- whether Defendants properly informed Class members that it captured, collected, used, and stored their biometric identifiers and/or biometric information;
- whether Defendants obtained "informed written consent" (740 ILCS 14/10) to capture, collect, use, and store Class members' biometric identifiers and/or biometric information;

[24] Pindrop Careers, https://www.pindrop.com/company/careers/, *archived at* https://perma.cc/99RC-RC4D (Pindrop advertises on its website that it offers "health and wellness" benefits including medical coverage, requiring the collection of employees' healthcare data, and AWS, similarly, offers health benefits to certain employees and collects employee healthcare data).

- whether Defendants developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and/or biometric information;
- whether Defendants disseminated Class members' biometric identifiers and/or biometric information;
- whether Defendants profited from Class members' biometric identifiers and/or biometric information;
- whether Defendants used Class members' biometric identifiers and/or biometric information to identify them; and
- whether Defendants' violations of BIPA were committed recklessly or negligently.

127. Predominance. These common questions of law and fact predominate over any individual issue that may arise on behalf of an individual Class member.

128. Typicality. Plaintiffs, the members of the Class, and Defendants have a commonality of interest in the subject matter of the lawsuit and the remedy sought.

129. Adequacy. Plaintiffs and counsel will fairly and adequately protect the interests of Class members. Plaintiffs' lead counsel, Schlichter Bogard & Denton, LLP, will fairly and adequately represent the interests of the Class and is best able to represent the interests of the Class under Rule 23(g). Schlichter Bogard & Denton has been appointed as lead class counsel in dozens of class actions. Federal courts and others have consistently and repeatedly recognized the firm's success:

- "This Court is unaware of any comparable achievement of public good by a private lawyer in the face of such obstacles and enormous demand of resources and finance." Order on Attorney's Fees, *Mister v. Illinois Central Gulf R.R.*, No. 81-3006 (S.D. Ill. 1993).
- "Schlichter, Bogard & Denton has achieved unparalleled results on behalf of its clients, . . . has invested . . . massive resources and persevered in the face of . . . enormous risks[.]" *Nolte v. Cigna Corp.*, No. 07-2046, 2013 WL 12242015, at *2 (C.D. Ill. Oct. 15, 2013).

- "Of special importance is the significant, national contribution made by the Plaintiffs whose litigation clarified ERISA standards in the context of investment fees. The litigation educated plan administrators, the Department of Labor, the courts and retirement plan participants about the importance of monitoring recordkeeping fees and separating a fiduciary's corporate interest from its fiduciary obligations." *Tussey v. ABB, Inc.*, No. 06-4305, 2015 WL 8485265 at *2 (W.D. Mo. Dec. 9, 2015).

- "Class Counsel's efforts have not only resulted in a significant monetary award to the class but have also brought improvement to the manner in which the Plans are operated and managed which will result in participants and retirees receiving significant savings[.]" *Kruger v. Novant Health, Inc*., No. 14- 208, Doc. 61, at 7–8 (M.D.N.C. Sept. 29, 2016).

- "[Schlichter Bogard & Denton achieved an] outstanding result for the class," and "demonstrated extraordinary resourcefulness, skill, efficiency and determination." *Gordan v. Mass Mutual Life Ins., Co.*, No. 14-30184, Doc. 144 at 5 (D. Mass. Nov. 3, 2016).

- "[Schlichter, Bogard & Denton] pioneered this ground-breaking and novel area of litigation" that has "dramatically brought down fees in defined contribution plans." *Kelly v. Johns Hopkins Univ.*, No. 1:16-CV-2835-GLR, 2020 WL 434473, at *2 (D. Md. Jan. 28, 2020).

- The firm's class action work has been featured in the New York Times, Wall Street Journal, NPR, Reuters, and Bloomberg, among other media outlets. *See, e.g.*, Anne Tergesen, *401(k) Fees, Already Low, Are Heading Lower*, Wall St. J. (May 15, 2016);[25] Gretchen Morgenson, *A Lone Ranger of the 401(k)'s*, N.Y. Times (Mar. 29, 2014);[26] Liz Moyer, *High Court Spotlight Put on 401(k) Plans*, Wall St. J. (Feb. 23, 2015);[27] Floyd Norris, *What a 401(k) Plan Really Owes Employees*, N.Y. Times (Oct. 16, 2014);[28] Sara Randazzo, *Plaintiffs'*

[25] Anne Tergesen, *401k Fees, Already Low, Are Heading Lower*, Wall Street Journal (May 15, 2016), http://www.wsj.com/articles/401-k-fees-already-low-are-heading-lower-1463304601, *archived at* https://perma.cc/T4KY-QVCT.

[26] Gretchen Morgensen, *A Lone Ranger of the 401(k)'s*, New York Times (Mar. 29, 2014), http://www.nytimes.com/2014/03/30/business/a-lone-ranger-of-the-401-k-s.html?_r=0, *archived at* https://perma.cc/5ZGL-XCJY.

[27] Liz Moyer, *High-Court Spotlight Put on 401(k) Plans*, Wall Street Journal (Feb. 23, 2015), http://www.wsj.com/articles/high-court-spotlight-put-on-401-k-plans-1424716527, *archived at* https://perma.cc/Z878-LH5R.

[28] Floyd Norris, *What a 401(k) Plan Really Owes Employees*, New York Times (Oct. 16, 2014), http://www.nytimes.com/2014/10/17/business/what-a-401-k-plan-really-owes-employees.html?_r=0, *archived at* https://perma.cc/RN8S-9ARU.

Lawyer Takes on Retirement Plans, Wall St. J. (Aug. 25, 2015);[29] Jess Bravin and Liz Moyer, *High Court Ruling Adds Protections for Investors in 401(k) Plans*, Wall St. J. (May 18, 2015); [30] Jim Zarroli, *Lockheed Martin Case Puts 401(k) Plans on Trial*, NPR (Dec. 15, 2014);[31] Mark Miller, *Are 401(k) Fees Too High? The High-Court May Have an Opinion*, Reuters (May 1, 2014);[32] Greg Stohr, *401(k) Fees at Issue as Court Takes Edison Worker Appeal*, Bloomberg (Oct. 2, 2014).[33]

130. Superiority. A class action is the appropriate vehicle for fair and efficient adjudication of Plaintiffs' and Class members' claims because if individual actions were required to be brought by each member of the Class, the result would be a multiplicity of actions, creating a hardship to the Class, to the Court, and to Defendants.

COUNT I – VIOLATION OF 740 ILCS 14/15(a)

131. Plaintiffs incorporate paragraphs 1 through 130 as though fully realleged herein.

132. BIPA created statutory duties for Defendants with respect to the possession of the biometric identifiers and biometric information of Plaintiffs and the Class. *See* 740 ILCS 14/15(a).

133. Defendants violated BIPA section 15(a) by possessing Plaintiffs' and Class members' biometric information, including voiceprints and related biometric information,

---

[29] Sara Randazzo, *Plaintiffs' Lawyer Takes On Retirement Plans*, Wall Street Journal (Aug. 25, 2015), http://blogs.wsj.com/law/2015/08/25/plaintiffs-lawyer-takes-on-retirement-plans/, *archived at* https://perma.cc/GPR3-2K8F.

[30] Jess Bravin and Liz Moyer, *High Court Ruling Adds Protections for Investors in 401(k) Plans*, Wall Street Journal (May 18, 2015), http://www.wsj.com/articles/high-court-ruling-adds-protections-for-investors-in-401-k-plans-1431974139, *archived at* https://perma.cc/2B5A-D4GQ.

[31] Jim Zarroli, *Lockheed Martin Case Puts 401(k) Plans On Trial*, National Public Radio (Dec. 15, 2014), http://www.npr.org/2014/12/15/370794942/lockheed-martin-case-puts-401-k-plans-on-trial, *archived at* https://perma.cc/4ANG-CYJS.

[32] Mark Miller, *Are 401(k) fees too high? The high court may have an opinion*, Reuters (May 1, 2014), http://www.reuters.com/article/us-column-miller-401fees-idUSBREA400J220140501, *archived at* https://perma.cc/WP3H-YJ3H.

[33] Greg Stohr, *401(k) Fees at Issue as Court Takes Edison Worker Appeal*, Bloomberg Business (Oct. 2, 2014), http://www.bloomberg.com/news/articles/2014-10-02/401-k-fees-at-issue-as-court-takes-edison-worker-appeal, *archived at* https://perma.cc/DR9Y-3VJN.

without creating and following a written policy, made available to the public, establishing and following a retention schedule and destruction guidelines for their possession of biometric identifiers and information.

134. Defendants' BIPA violations are violations of Defendants' duty of ordinary care owed to Plaintiffs and the Class.

135. In the alternative, Defendants' BIPA violations were willful and wanton. Defendants knowingly, intentionally and/or recklessly violated the duty they owed to Plaintiffs and the Class.

136. Plaintiffs incurred injuries that were proximately caused by Defendants' conduct. Through their actions, Defendants exposed Plaintiffs and the Class to imminent threats of serious harm.

137. Plaintiffs in this Count II hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

COUNT II – VIOLATION OF 740 ILCS 14/15(b)

138. Plaintiffs incorporate paragraphs 1 through 137 as though fully realleged herein.

139. BIPA created statutory duties for Defendants with respect to the collection of biometric identifiers and biometric information of Plaintiffs and the Class. *See* 740 ILCS 14/15(b).

140. Defendants violated BIPA section 15(b)(1) by capturing, collecting, and obtaining Plaintiffs' and Class members' biometric identifiers and biometric information, including voiceprints and related biometric information, without first informing Plaintiffs and Class members that they were collecting this information.

141. Defendants violated BIPA section 15(b)(2) by capturing, collecting and obtaining Plaintiffs' and Class members' biometric identifiers and biometric information, including voiceprints and related biometric information, without informing Plaintiffs and Class members in writing of the purpose for the collection. Further, Defendants violated BIPA section 15(b)(2) by failing to inform Plaintiffs and Class members in writing of the length of time Defendants would store and use Plaintiffs' and Class members' biometric identifiers and biometric information, including voiceprints and related biometric information.

142. Defendants violated BIPA section 15(b)(3) by capturing, collecting and obtaining Plaintiffs' and Class members' biometric identifiers and biometric information, including voiceprints and related biometric information, without first obtaining informed written consent authorizing Defendants to capture or collect Plaintiffs' and Class members' biometric identifiers and/or biometric information.

143. Defendants' BIPA violations are violations of Defendants' duty of ordinary care owed to Plaintiffs and the Class.

144. In the alternative, Defendants' BIPA violations were willful and wanton. Defendants knowingly, intentionally, and/or recklessly violated the duty they owed to Plaintiffs and the Class.

145. Plaintiffs incurred injuries that were proximately caused by Defendants' conduct. Through their actions, Defendants exposed Plaintiffs and the Class to imminent threats of serious harm.

146. Plaintiffs in this Count II hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

COUNT III – VIOLATION OF 740 ILCS 14/15(c)

147. Plaintiffs incorporate paragraphs 1 through 146 as though fully realleged herein.

148. Under BIPA, Defendants owed a duty to Plaintiffs and the Class not to profit from their Biometric Data. *See* 740 ILCS 14/15(c).

149. Defendants are subject to BIPA section 15(c) because they are "private entit[ies] in possession of a biometric identifier or biometric information."

150. Defendants violated BIPA section 15(c) by profiting from the possession of Plaintiffs' and Class members' biometric identifiers and biometric information, including voiceprints and related biometric information, by among other things, marketing, selling and performing biometric analysis and storage services that included collecting and possessing Plaintiffs' Biometric Data.

151. Defendants' BIPA violations are violations of Defendants' duty of ordinary care owed to Plaintiffs and the Class.

152. In the alternative, Defendants' BIPA violations were willful and wanton. Defendants knowingly, intentionally and/or recklessly violated the duty they owed to Plaintiffs and the Class.

153. Plaintiffs incurred injuries that were proximately caused by Defendants' conduct. Through their actions, Defendants exposed Plaintiffs and the Class to imminent threats of serious harm.

154. Plaintiffs in this Count III hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

COUNT IV – VIOLATION OF 740 ILCS 14/15(d)

155. Plaintiffs incorporate paragraphs 1 through 154 as though fully realleged herein.

156. Defendants violated BIPA section 15(d) by disclosing, redisclosing, and disseminating Plaintiffs' and Class members' biometric identifiers and biometric information, including voiceprints and related biometric information, without consent, and despite that the disclosure, redisclosure, and dissemination was not necessary to complete any financial transaction requested or authorized by Plaintiffs and Class members.

157. Defendants' BIPA violations are violations of Defendants' duty of ordinary care owed to Plaintiffs and the Class.

158. In the alternative, Defendants' BIPA violations were willful and wanton. Defendants knowingly, intentionally and/or recklessly violated the duty they owed to Plaintiffs and the Class.

159. Plaintiffs incurred injuries that were proximately caused by Defendants' conduct. Through their actions, Defendants exposed Plaintiffs and the Class to imminent threats of serious harm.

160. Plaintiffs in this Count IV hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

COUNT V – VIOLATION OF 740 ILCS 14/15(e)

161. Plaintiffs incorporate paragraphs 1 through 160 as though fully realleged herein.

162. Defendants violated BIPA section 15(e)(1) by possessing Plaintiffs' and Class members' biometric identifiers and biometric information, including voiceprints and related biometric information, but failing to store, transmit, and protect from disclosure these biometric

identifiers and biometric information while using a reasonable standard of care within Defendants' respective industries.

163. Defendants violated BIPA section 15(e)(2) by possessing Plaintiffs' and Class members' biometric identifiers and biometric information, including voiceprints and related biometric information, but failing to store, transmit, and protect these biometric identifiers and biometric information in a manner the same as or more protective than the manner in which Defendants store, transmit, and protect other confidential and sensitive information, including, but not limited to healthcare data.

164. Defendants' BIPA violations are violations of Defendants' duty of ordinary care owed to Plaintiffs and the Class.

165. In the alternative, Defendants' BIPA violations were willful and wanton. Defendants knowingly, intentionally and/or recklessly violated the duty they owed to Plaintiffs and the Class.

166. Plaintiffs incurred injuries that were proximately caused by Defendants' conduct. Through their actions, Defendants exposed Plaintiffs and the Class to imminent threats of serious harm.

167. Plaintiffs in this Count V hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, pray for judgment against Defendants Amazon Web Services, Inc. and Pindrop Security, Inc. as follows:

A. Certifying this case as a class action, appointing Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Finding that Defendants' conduct violates BIPA;

C. Awarding actual damages caused by Defendants' BIPA violations;

D. Awarding statutory damages of $5,000 for each intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1);

E. Awarding injunctive and/or other equitable or non-monetary relief as appropriate to protect the Class, including by enjoining Defendants from further violating BIPA pursuant to 740 ILCS 14/20(4);

F. Awarding Plaintiffs reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);

G. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

H. Awarding such other and further relief as this Court deems appropriate and as equity and justice may require.

JURY DEMAND

Plaintiffs request trial by jury of all claims asserted herein.

October 16, 2020

BAYARD, P.A.

/s/ Stephen B. Brauerman

Andrew D. Schlichter
Joel Rohlf
Alexander L. Braitberg
SCHLICHTER BOGARD & DENTON LLP
100 South Fourth St., Ste. 1200
St. Louis, MO 63102
Phone: (314) 621-6115
Fax: (314) 621-5934
aschlichter@uselaws.com
jrohlf@uselaws.com
abraitberg@uselaws.com

Stephen B. Brauerman (#4952)
Ronald P. Golden III (#6254)
600 North King Street, Suite 400
Wilmington, Delaware 19801
(302) 655-5000
sbrauerman@bayardlaw.com
rgolden@bayardlaw.com

Attorneys for Plaintiffs