**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS**

CHRISTINE MCGOVERAN, JOSEPH VALENTINE, and AMELIA RODRIGUEZ, on behalf of themselves and all other persons similarly situated,	
Plaintiffs,	
v.	**Case No. 3:20-CV-31-NJR**
AMAZON WEB SERVICES, INC. and PINDROP SECURITY, INC.,	
Defendants.	

MEMORANDUM AND ORDER

ROSENSTENGEL, Chief Judge:

This matter is before the Court on the motions to dismiss filed by Defendants Pindrop Security, Inc. (Doc. 35) and Amazon Web Services, Inc. (Doc. 49). Defendants seek to dismiss the case for lack of personal jurisdiction under Federal Rule of Civil Procedure 12(b)(2). Alternatively, they move for dismissal under Rule 12(b)(6) for failure to state a claim. For the following reasons, this action is dismissed for lack of personal jurisdiction.

BACKGROUND

On December 17, 2019, Plaintiffs Christine McGoveran, Joseph Valentine, and Amelia Rodriguez filed a putative Class Action Complaint against Defendants Amazon Web Services, Inc. ("AWS"), and Pindrop Security, Inc. ("Pindrop"), in the Circuit Court for the Third Judicial Circuit in Madison County, Illinois, alleging violations of the

Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. § 14/1, *et seq*. (Doc. 1-1). Specifically, Plaintiffs allege Pindrop and AWS violated BIPA by collecting, possessing, redisclosing, profiting from, and failing to safeguard their biometric identifiers and biometric information, including their voiceprints (*Id.* at ¶ 1).

Voiceprinting, also known as voice biometrics, is the use of biological characteristics—one's voice—to verify an individual's identity without requiring the use of a passcode or answers to secret questions (*Id.* at ¶¶ 33-35). Unlike a traditional passcode, however, in the event of a data breach there is nothing the individual can do to prevent someone from using his or her voiceprint to gain access to a compromised account (*Id.* at ¶ 36).

Plaintiffs allege Pindrop offers voiceprint services for use by call centers and customer service personnel to confirm the identity of callers (*Id.* at ¶¶ 38-39). Pindrop does this through its "Deep Voice" product, which uses biometrics to identify and analyze repeat callers (*Id.* at ¶ 42). Similarly, Pindrop's "Phoneprinting" product analyzes call audio to create a distinctive identifier for each caller (*Id.*).

AWS offers cloud storage services, including the ability for customers to store their data, access data remotely, and create backup copies of data (*Id.* at ¶ 45). AWS also offers call center services under the brand "Amazon Connect" (*Id.* at ¶ 46). In connection with Amazon Connect, AWS possesses and stores a variety of types of customer data, including biometric identifiers and information (*Id.* at ¶¶ 48-49).

Pindrop was one of the first partners with AWS in launching Amazon Connect (*Id.* at ¶ 52). Plaintiffs allege that after an individual places a call to an AWS client's call center, the audio is sent to Pindrop for processing (*Id.* at ¶¶ 57-59; Doc. 57 at p. 8). Pindrop then processes the audio, analyzes the caller's unique voice biometric data, and sends the results of its analysis to AWS's servers (*Id.* at ¶¶ 58-59; Doc. 57 at p. 8). Plaintiffs claim that once this process occurs, AWS then possesses "biometric information" as defined by BIPA (*Id.* at. ¶ 60).

With regard to the named Plaintiffs, the Complaint alleges that they called John Hancock customer service representatives or call centers on numerous occasions regarding investment or insurance products (*Id.* at ¶¶ 67-70; Doc. 57 at p. 9). Plaintiffs were residents of Illinois, located in Illinois, and used Illinois phone numbers to call John Hancock (Docs. 57-2; 57-3; 57-4). John Hancock's call centers use Amazon Connect with Pindrop biometric voiceprint authentication; as a result, they no longer require customers to have a pin number for authentication (*Id.* at ¶¶ 71-72). Plaintiffs allege that AWS and Pindrop apply their voice biometric technology to every caller to John Hancock's call centers (*Id.* at ¶ 73).

Plaintiffs' Complaint asserts five counts of BIPA violations, 740 ILL. COMP. STAT. § 14/15(a)-(e). In Count I, Plaintiffs claim that Defendants violated BIPA section 14/15(a) by possessing Plaintiffs' and Class members' biometric information, including voiceprints and related biometric information, 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 (*Id.* at ¶ 90). In Count II, Plaintiffs assert Defendants violated BIPA section 14/15(b) by failing to inform John Hancock's Illinois callers that their biometric information is being collected and stored and by not obtaining any form of consent (*Id.* at ¶¶ 94-95). In Count III, Plaintiffs allege that Defendants violated BIPA section 14/15(c) by profiting from the possession of their biometric information, including their voiceprints (*Id.* at ¶ 102). Count IV alleges Defendants violated BIPA section 14/15(d) when they disclosed, redisclosed, and disseminated their biometric information, including voiceprints, without consent (*Id.* at ¶ 107). Finally, Plaintiffs claim Defendants violated BIPA section 14/15(e) by failing to use reasonable care in storing, transmitting, and protecting the biometric information from disclosure, or by failing to do so in a manner the same as or more protective than the manner in which Defendants store, transmit, and protect other confidential and sensitive information (*Id.* at ¶¶ 112-13).

Plaintiffs seek to represent a class consisting of:

> 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.

(*Id.* at ¶ 81).

On behalf of themselves and the putative class, Plaintiffs seek an order enjoining Defendants from further violating BIPA, actual damages, statutory damages of $5,000 for each intentional and reckless violation of BIPA pursuant to 740 ILL. COMP. STAT. 14/20(2), or statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILL. COMP. STAT. 14/20(1), attorneys' fees and costs, and pre- and post-judgment interest. 740 ILL. COMP. STAT. 14/20(3). (*Id.* at pp. 26-27).

Subject Matter Jurisdiction

On January 8, 2020, Defendants removed the action to this Court under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d)(2) (Doc. 1). CAFA extends federal jurisdiction over class actions where: (1) any member of the proposed class is a citizen of a state different from any defendant (*i.e.*, minimal diversity exists); (2) the proposed class consists of more than 100 members; and (3) the amount in controversy is $5,000,000 or more, aggregating all claims and exclusive of interest and costs. *See* 28 U.S.C. §§ 1332(d)(2), 1332(d)(5)(B).

Here, the proposed class consists of more than 100 members, as Plaintiffs allege that the putative class includes "thousands of people." (Doc. 1-1 at ¶ 82). There also is minimal diversity of citizenship between the parties. Plaintiffs are citizens of Illinois, AWS is a Delaware corporation with its principal place of business in Washington, and Pindrop is a Delaware corporation with its principal place of business in Georgia (Docs. 1, 8). Finally, CAFA's amount in controversy requirement is satisfied. At a minimum, Plaintiffs allege statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILL. COMP. STAT. 14/20(1). Plaintiffs then allege at least five separate BIPA violations in Count I-V and have asserted there are thousands of class members. Even assuming a class size of only 1,000, the Complaint alleges damages of at least $5,000,000. And when considering attorneys' fees and potential statutory damages of $5,000 for each intentional and reckless violation of BIPA, the amount in controversy well exceeds the required threshold.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you’re on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm’s cloud-native docket research platform finds what other services can’t. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**