IN THE SUPERIOR COURT OF WASHINGTON FOR KING COUNTY

MICHELE ROSATI,

Plaintiff,

v.

AMAZON.COM, INC., a Delaware corporation,

Defendant.

NO.

COMPLAINT FOR RELIEF PURSUANT TO 8 DELAWARE GENERAL CORPORATION LAW CODE SECTION 220 TO COMPEL INSPECTION OF BOOKS AND RECORDS

Plaintiff Michele Rosati ("Plaintiff") herein alleges, upon knowledge as to herself and her own actions, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1.1 In this action, Plaintiff seeks to enforce her right to inspect certain corporate books and records of defendant Amazon.com, Inc. ("Amazon" or the "Company"), a Delaware corporation, pursuant to title 8, section 220 of the Delaware General Corporation Law Code ("Section 220"). Plaintiff is a beneficial stockholder of the Company.

1.2 On September 22, 2020, Plaintiff sent an inspection demand to the Company (the "Inspection Demand"). The Inspection Demand complied with all the form and manner requirements of Section 220, including that it was accompanied by a power of attorney, an oath,

and proof of Plaintiff's current ownership of Amazon stock. The Company received the letter on September 23, 2020.[1]

1.3 In the Inspection Demand, Plaintiff explained that she wishes to investigate potential wrongdoing occurring at the Company, including potential breaches of fiduciary duty. Plaintiff has legitimate concerns as to whether Amazon violated the Illinois Biometric Information Privacy Act ("BIPA") and whether the Company was engaging in antitrust violations.

1.4 The Inspection Demand provided ample evidence of such possible wrongdoing and mismanagement at Amazon. Concerning BIPA, the Inspection Demand explained that Amazon had been developing facial recognition software for years and purchased International Business Machines Corporation's ("IBM") "Diversity in Faces" dataset in 2019 to improve this software. In developing this facial recognition software, Amazon collected, stored, and used individuals' biometric identifiers without ever informing those before, a direct violation of BIPA.

1.5 Regarding Amazon's anticompetitive violations, the Inspection Demand again contained detailed information how the Company uses third-party seller data it has access to as an effective middleman to develop its own competing suite of products. The Company then undercuts the third-party on price. Amazon's anticompetitive actions have led to investigations by, at a minimum: (i) the U.S. Congress; (ii) the European Union; (iii) the State of California; and (iv) the State of Washington. Accordingly, Plaintiff has ample reason to suspect wrongdoing at Amazon, more than satisfying the credible basis standard necessary to justify the inspection.

1 True and correct copies of the Inspection Demand and proof of delivery are attached hereto as Exhibit A and B, respectively.

1.6 On October 19, 2020, the Company's counsel responded to Plaintiff's Inspection Demand with a short perfunctory two-and-a-half-page rejection. The rejection letter did; however, state Amazon was willing to discuss making a production to Plaintiff.

1.7 Over the next three months, Plaintiff attempted to reach a resolution with the Company. Unfortunately, Amazon steadfastly insisted on including in a nondisclosure agreement draconian terms that would prevent Plaintiff from bringing certain of her claims derivatively and otherwise waiving her rights. Despite providing directly on point authority that Amazon's position was untenable and contrary to the law, it did not move. Further, Amazon never stated what documents it was willing to allow Plaintiff to inspect.

1.8 On February 1, 2021, Amazon stated that it would "follow up" with Plaintiff that week about her Inspection Demand. Instead, she has been met with silence. It has now been approximately six months since Plaintiff sent the Inspection Demand and she is apparently no closer to reviewing the demanded books and records. Amazon's actions have effectively denied Plaintiff her statutory rights.

1.9 In light of Amazon's effective refusal, Plaintiff now respectfully asks the Court to order Amazon to produce the demanded books and records that she is entitled to review as a stockholder of the Company.

II. JURISDICTION AND VENUE

2.1 This Court retains general jurisdiction over each named defendant who is a resident of Washington. Additionally, this Court has specific jurisdiction over each named nonresident defendant because these defendants maintain sufficient minimum contacts with Washington to render jurisdiction by this Court permissible under traditional notions of fair play

and substantial justice. Amazon is headquartered in Washington. Finally, exercising jurisdiction over any nonresident defendant is reasonable under these circumstances.

2.2 Venue is proper in this Court because defendant Amazon maintains executive offices in this County, a substantial portion of the transactions and wrongs complained of herein, including the defendant's primary participation in the wrongful acts detailed herein occurred in this County, and defendant has received substantial compensation in this County by doing business here and engaging in numerous activities that had an effect in this County.

III. THE PARTIES

3.1 Plaintiff Michele Rosati is an owner of Amazon's common stock.

3.2 Defendant Amazon is a Delaware corporation with principal executive offices located at 410 Terry Avenue North, Seattle, Washington.

IV. THE COMPANY'S UNAUTHORIZED COLLECTION OF INDIVIDUALS' INFORMATION VIOLATES THE LAW

Biometrics and Facial Recognition Technology

4.1 Biometrics is the technical term for measurements used to identify people's unique physical characteristics. Examples of biometric identifiers include an individual's DNA, fingerprints, irises or retinas, voiceprints, and facial geometry. The uniqueness and potential permanence of biometric identifiers present an advantage for businesses to accurately identify and distinguish individuals. Businesses presently use biometrics in a wide variety of applications, including data collection.

4.2 One technological application of biometrics is facial recognition software. Facial recognition software uses biometrics to map facial features from a photograph or video. In particular, the software uses an algorithm that calculates a unique digital representation of the face based on the geometric relationship of a person's facial features (such as the distance

between their eyes, ears, and nose), creating a face signature or map. The software then compares the information with a database of known faces to find a match.

4.3 Facial recognition technology has seen steady improvement over the past decade. Lower costs and increased accuracy have allowed companies such as Amazon to deploy increasingly sophisticated facial recognition software in their applications. However, this increased sophistication has raised serious privacy concerns. Biometrics present potential privacy threats to the individual if compromised, such as a heightened risk for identity theft. During a U.S. Senate hearing in 2012 on the use of facial recognition technology, Senator Al Franken noted that "[o]nce someone has your faceprint, they 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 Government buildings you enter, and the photos your friends post online." He added, "facial recognition technology can allow others to access all of that information from a distance, without your knowledge and in about as much time as it takes to snap a photo." Faceprints can even be used to identify protesters at political rallies and "target them for selective jailing and prosecution, stifling their First Amendment rights."

4.4 The U.S. Federal Trade Commission ("FTC") has also noted the public's concerns over privacy in social networks that "databases of photos or biometric data may be susceptible to breaches and hacking." The FTC urged companies using facial recognition technology to ask for consent *before* collecting biometric information from a photo. In its best practices guidelines, the FTC addressed social networks in particular, stating, "before using facial recognition to identify an individual it could not otherwise identify, the company should obtain the affirmative express consent of the individual in the image."

/ / /

DOCKET ALARM

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.