1

2

3

4 UNITED STATES DISTRICT COURT

5 NORTHERN DISTRICT OF CALIFORNIA

6

7 BRANDON BRISKIN,

8   Plaintiff,

     Case No. 21-cv-06269-PJH

9   v.

     ORDER OF DISMISSAL

10 SHOPIFY INC., et al.,

     Re: Dkt. Nos. 51, 52, 53

11   Defendants.

12

13

14   The three motions of defendants Shopify Inc., Shopify (USA) Inc., and Shopify

15 Payments (USA) Inc. to dismiss plaintiff's second amended complaint ("SAC") all came

16 on for hearing before this court on April 28, 2022. Plaintiff appeared through his counsel,

17 Kali Backer. Defendants appeared through their counsel, Aravind Swaminathan and

18 Thomas Fu. Having read the papers filed by the parties and carefully considered their

19 arguments and the relevant legal authority, and good cause appearing, the court hereby

20 rules as follows.

21   **BACKGROUND**

22   This putative class action for invasion of privacy concerns the collection of

23 consumer data over an online shopping platform. Plaintiff Brandon Briskin is an Internet

24 shopper and resident of Madera, California. SAC ¶ 8. Defendant Shopify Inc. is a

25 Canadian company headquartered in Ottawa, Canada. SAC ¶ 9. Defendant Shopify

26 (USA) Inc. ("Shopify USA") is a Delaware company with its principal place of business in

27 Ottawa, Canada. SAC ¶ 14. Defendant Shopify Payments (USA) Inc. ("Shopify

Payments") is a Delaware company with its principal place of business in Wilmington,

United States District Court
Northern District of California

1   Delaware. SAC ¶ 15. Both Shopify USA and Shopify Payments are wholly owned

2   subsidiaries of Shopify Inc. Plaintiff refers to the three defendants repeatedly and

3   collectively throughout the SAC as "Shopify."

A.   Allegations of defendants' conduct with consumer data

5   Defendants run an e-commerce platform that provides payment processing

6   services to millions of merchants across the Internet. SAC ¶ 24. Defendants host

7   merchants' websites in addition to facilitating and verifying customers' payment

8   information. SAC ¶ 24. Plaintiff alleges that when a consumer begins the checkout

9   process with one of Shopify's merchant customers, the software makes it appear that the

10   consumer communicates directly with the merchant, but in reality, the consumer does not

11   send any information to the merchant. SAC ¶¶ 1-2, 4, 25-35, 82. Rather, Shopify's

12   software generates the payment form and collects all information entered into it. Id.

13   Plaintiff complains that Shopify also installs cookies on users' browsers to track

14   consumers' transactions across the Shopify merchant network. SAC ¶¶ 5, 38-41.

15   In June 2019, plaintiff purchased fitness apparel from IABMFG, a Shopify Inc.

16   merchant, through IABMFG's website. SAC ¶ 57. Plaintiff alleges that he, like other

17   consumers, was uninformed of defendants' conduct, and without consent, defendants

18   collected sensitive private information, including consumers' full names, addresses, email

19   addresses, credit card numbers, IP addresses, the items purchased, and geolocation.

20   SAC ¶¶ 2-3, 40, 81. In defendants' course of collecting the data, they can decipher what

21   data emanates from California because they have consumers' billing addresses and

22   geolocations. Id. Defendants take additional steps to use consumer data and make it

23   profitable for themselves and their merchants by compiling the data into individualized

24   profiles. SAC ¶¶ 6, 42-45. Defendants share information within the profiles of

25   consumers with their merchants. Id. The information is valuable to the merchants

26   because they provide insights into consumers' creditworthiness before the transaction is

27   final. Id.

United States District Court
Northern District of California

1   When a consumer makes a purchase, defendants use the consumer's data to

2   provide their merchants with an "analysis" of the order that cross-references the details of

3   the new transaction with the consumer's purchase history to identify potential areas of

4   fraud. SAC ¶ 43. In addition to building profiles and analyzing their data, defendants

5   share consumer data with other non-merchant third-parties, such as Stripe and MaxMind,

6   who, in turn, use the data to feed their own profiles on consumers. SAC ¶¶ 15-16, 46-47.

7   **B.   Shopify's Contacts with California**

8   Plaintiff alleges that Shopify's efforts to drive Internet-based sales in California go

9   beyond simply making its software available for use by California companies—Shopify

10   actively courts California merchants who it knows are doing business with California

11   consumers. For instance, in 2017, Shopify built Kylie Cosmetics, one of its largest online

12   merchants, a pop-up store in Los Angeles with the goal of learning more about its base of

13   consumers. SAC ¶ 10. Shopify sent members of its own team as well as hired an

14   agency to secure workers to run the store. Id.   In 2018, Shopify deepened its ties with

15   California when it opened a physical store in Los Angeles to serve as a hub where its

16   merchants can learn about its products and receive "business advice" and "learn about

17   the company's online platform." SAC ¶¶ 11-12. As of 2018, California was home to over

18   80,000 Shopify merchants with 10,000 in Los Angeles alone. SAC ¶ 11-12.

19   **C.   Plaintiff's Claims**

20   Plaintiff alleges that he never granted consent for defendants to collect and use his

21   data in the methods described above, and he seeks to represent a class of similarly

22   situated consumers. His proposed class definition is as follows: "All natural persons who,

23   between August 13, 2017 and the present, submitted payment information via Shopify's

24   software while located in California." SAC ¶ 68. The SAC brings the following claims on

25   behalf of plaintiff and the proposed class against all three defendants, all under California

26   law:

27   1. Violation of the California Invasion of Privacy Act, California Penal Code § 631;

3. Invasion of Privacy Under California's Constitution;

4. Intrusion Upon Seclusion;

5. Violation of the California Computer Data Access and Fraud Act, Cal. Penal Code § 502; and

6. Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq.

D.   Procedural History

The original complaint was filed on August 13, 2021, naming only Shopify Inc. and Shopify USA. Dkt. 1. Before defendants responded, plaintiff filed a first amended complaint on October 29, 2021. Dkt. 17. Defendants filed separate motions to dismiss in response on December 8, 2021. Dkt. 29 and 30. Rather than opposing the motions, plaintiff sought leave of court to file a second amended complaint, which defendants opposed. Dkt. 36-40. The court granted plaintiff leave to file, and plaintiff filed, the now-operative second amended complaint, which added Shopify Payments and added some allegations intended to address defects highlighted by defendants' prior motions. Dkt. 43 and 44.

In response to the second amended complaint, the three defendants filed the instant motions to dismiss. Dkt. 51, 52, and 53. All three defendants ask the court to dismiss the complaint pursuant to Federal Rule of Civil Procedure 8(a)(2) for failure to provide adequate notice of the claims against them, or in the alternative, pursuant to Federal Rule 12(b)(2) for lack of personal jurisdiction, or in the further alternative, pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted.

DISCUSSION

From the several grounds for dismissal offered in defendants' moving papers, the court focuses on only two grounds for dismissal: (1) whether the SAC comports with the pleading requirements of Rule 8 and (2) whether the court may exercise jurisdiction over

A.   Sufficiency of Pleading

1.   Legal Standard

A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) tests for the legal sufficiency of the claims alleged in the complaint. Ileto v. Glock Inc., 349 F.3d 1191, 1199-1200 (9th Cir. 2003). Under Federal Rule of Civil Procedure 8, which requires that a complaint include a "short and plain statement of the claim showing that the pleader is entitled to relief," Fed. R. Civ. P. 8(a)(2), a complaint may be dismissed under Rule 12(b)(6) if the plaintiff fails to state a cognizable legal theory, or has not alleged sufficient facts to support a cognizable legal theory. Somers v. Apple, Inc., 729 F.3d 953, 959 (9th Cir. 2013). "A complaint which lumps together multiple defendants in one broad allegation fails to satisfy the notice requirement of Rule 8(a)(2)." Adobe Sys. Inc. v. Blue Source Grp., Inc., 125 F. Supp. 3d 945, 964 (N.D. Cal. 2015) (cleaned up).

As a general rule, "Plaintiffs' failure to allege what role each Defendant played in the alleged harm makes it exceedingly difficult, if not impossible, for individual Defendants to respond to Plaintiffs' allegations." In re iPhone Application Litig., No. 11-MD-02250-LHK, 2011 WL 4403963, at *8 (N.D. Cal. Sept. 20, 2011) (Koh, J.). Accordingly, a complaint that lumps multiple defendants together in broad allegations falls short of providing the necessary notice under Rule 8(a)(2). Gen-Probe, Inc. v. Amoco Corp., 926 F. Supp. 948, 961 (S.D. Cal.1996). Put another way, a plaintiff's allegations must "provide sufficient notice to all of the Defendants as to the nature of the claims being asserted against them," including "what conduct is at issue." Villalpando v. Exel Direct Inc., No. 12-CV-04137 JCS, 2014 WL 1338297, at *5 (N.D. Cal. Mar. 28, 2014).

2.   Analysis

Here, plaintiff admittedly alleges all claims against all three defendants without distinguishing the conduct of any single entity, referring collectively to "Shopify." SAC ¶ 18. Plaintiff contends that the three related entities are sufficiently put on notice of the

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.

fastcase®
Smarter legal research.