1

2

3

4   UNITED STATES DISTRICT COURT

5   NORTHERN DISTRICT OF CALIFORNIA

6

7   EDWARD BATON, et al.,   Case No. 21-cv-02470-EMC

8   Plaintiffs,

9   v.   **ORDER GRANTING DEFENDANTS'**
                                              MOTIONS TO DISMISS
10   LEDGER SAS, et al.,   Docket Nos. 55, 56, 58

11   Defendants.

12

13

14   **I.   INTRODUCTION**

15   Plaintiffs, customers who purchased a hardware wallet to protect cryptocurrency assets,

16   bring a putative class action seeking redress for harms they allegedly suffered stemming from a

17   data breach exposing over 270,000 pieces of personally identifiable information, including

18   customer names, email addresses, postal addresses and telephone numbers. Docket No. 33 (First

19   Amended Complaint or "FAC"). Now pending before the Court are Defendants Shopify USA,

20   Shopify, Inc. and Ledger's respective motions to dismiss the complaint for, among other reasons,

21   lack of personal jurisdiction. Docket Nos. 55, 56, 58.

22   For the following reasons, the Court finds that it lacks personal jurisdiction over each

23   defendant and that jurisdictional discovery is unwarranted. Therefore, the Court **GRANTS** the

24   motions to dismiss and dismisses the case with prejudice.

25   **II.   BACKGROUND**

26   A.   Summary of Allegations in the FAC

27   Plaintiffs are customers of Defendant Ledger SAS ("Ledger"), a French company based in

("FAC") ¶ 2, 21. Ledger sells its hardware wallets—the Ledger Nano X and Ledger Nano S—through its e-commerce website, which operates on Defendant Shopify, Inc.'s platform. FAC ¶¶ 2, 16-17. Plaintiffs allege they, and several putative classes, each bought a Ledger hardware wallet on Ledger's e-commerce website, through Shopify's platform, between July 2017 and June 2020. *Id.* ¶¶ 16-20. When Plaintiffs made their purchases, they provided their name, email addresses, telephone numbers and postal addresses. *Id.*

Plaintiffs' claims arise of two security incidents involving data breaches exposing Plaintiffs' contact information. FAC ¶¶ 78, 79, 88. First, Plaintiffs allege that between April and June 2020, rogue Shopify, Inc. employees exported a trove of data, including Ledger's customer transactional records. *Id.* ¶¶ 78-79. Shopify allegedly publicly announced the theft on September 22, 2020, which involved the data of approximately 272,000 people. *Id.* ¶¶ 79, 82. Plaintiffs allege that Ledger did not inform them that their data was involved in the Shopify breach at that time. *Id.* ¶ 83. Second, Plaintiffs allege that Ledger publicly announced that an unauthorized third-party gained access to Ledger's e-commerce database through an application programming interface key on June 25, 2020 and acquired the email addresses of one million customers and physical contact information of 9,500 customers. *Id.* ¶ 88. Plaintiffs allege that Ledger did not disclose that the attack on Ledger's website and the theft of Shopify's data were connected, that Ledger downplayed the scale of the actual attack, and, as a result, Plaintiffs and putative class members were subject to phishing scams, cyber-attacks, and demands for ransom and threats. *Id.* ¶¶ 95-118. Plaintiffs contend that Ledger knew that its customer list was highly valuable to hackers, because it was a list of people who have converted substantial wealth into anonymized crypto-assets that are transferrable without a trace. *Id.* ¶ 5.

Plaintiffs allege that despite knowing the high value of its customer list and the need for confidentiality, Ledger did not implement security measures to protect its customers by regularly deleting and/or archiving the customer data to protect that information from online accessibility. FAC ¶ 136, and that Ledger failed to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting its customers personal information that Ledger had in its

1   unauthorized persons, *id.* ¶ 117. Similarly, Plaintiffs allege Shopify failed to exercise reasonable

2   care in obtaining, retaining, securing, safeguarding, deleting, and protecting their personal

3   information in their possession from being compromised, lost, or stolen, and from being accessed,

4   and misused by unauthorized persons. FAC ¶¶ 78-83.

5   Plaintiffs are five Ledger customers who reside, respectively, in California, Georgia, New

6   York, London, United Kingdom and Tel Aviv, Israel. *Id.* ¶¶ 26-20. They purport to represent

7   several classes and subclasses, ranging from customers internationally to customers in particular

8   states who suffered particular harms. *Id.* ¶ 145. Plaintiffs bring claims for, among others,

9   negligence, negligence per se, injunctive relief and remedies under California's unfair competition

10   law, Georgia's Fair Business Practices Act and New York's General Business Law. *Id.* ¶¶ 168-

11   276.

12   B.   Relevant Factual Background Contained in Jurisdictional Declarations

13   Defendants include additional factual background relevant to the Court's jurisdictional

14   inquiries at the motion to dismiss stage. Shopify USA states that it is incorporated in Delaware,

15   has its principal place of business in Ontario, Canada, and never had a business relationship with

16   Ledger. Docket No. 55-1 ("Harris-John Decl.") ¶¶ 3-6. Shopify Inc., explains it is a Canadian

17   corporation that it is not registered to do business in California and, does not have any employees

18   in California. Docket No. 56-1 ("McIntomny Decl.") ¶¶ 2-5. It explains that the "rogue"

19   individuals who were responsible for the data breach of Shopify, Inc.'s platform were not

20   employees of Shopify or any of its affiliated companies, but independent contractors of a company

21   called TaskUs, who were located in the Philippines. *Id.* ¶¶ 11-12. Ledger explains that it is a

22   French company with no California or U.S. employees. Docket No. 59 ("Ricomard Decl.") ¶¶ 5,

23   11, 17.

24   C.   Procedural Background

25   Defendant Ledger Technologies was voluntarily dismissed from this case. Docket No. 36.

26   Remaining Defendants Shopify USA, Shopify, Inc. and Ledger move to dismiss Plaintiffs' First

27   Amended Complaint on multiple grounds, including for lack of personal jurisdiction and failure to

1   **III.   LEGAL STANDARD**

2   A.   Federal Rule of Procedure 12(b)(2)

3   A defendant may move to dismiss based on lack of personal jurisdiction pursuant to

4   Federal Rule of Civil Procedure 12(b)(2).

5   In opposing a defendant's motion to dismiss for lack of personal
         jurisdiction, the plaintiff bears the burden of establishing that
6   jurisdiction is proper. Where, as here, the defendant's motion is
         based on written materials rather than an evidentiary hearing, the
7   plaintiff need only make a prima facie showing of jurisdictional
         facts to withstand the motion to dismiss. The plaintiff cannot
8   "simply rest on the bare allegations of its complaint," but
         uncontroverted allegations in the complaint must be taken as true.

9

10   *Mavrix Photo, Inc. v. Brand Techs., Inc.*, 647 F.3d 1218, 1223 (9th Cir. 2011); *see also Data Disc,*

11   *Inc. v. Sys. Tech. Assocs., Inc.*, 557 F.2d 1280, 1285 (9th Cir. 1977) (noting that "[t]he limits

12   which the district judge imposes on the pre-trial proceedings will affect the burden which the

13   plaintiff is required to meet"). In addition, all disputed facts are resolved in favor of the plaintiff.

14   *See Pebble Beach Co. v. Caddy*, 453 F.3d 1151, 1154 (9th Cir. 2006); *see also Freestream*

15   *Aircraft (Berm.) Ltd. v. Aero Law Grp.*, 905 F.3d 597, 602 (9th Cir. 2018) (stating that

16   "[u]ncontroverted allegations in the complaint must be taken as true, and factual disputes are

17   construed in the plaintiff's favor").

18   **IV.   DISCUSSION**

19   A.   Personal Jurisdiction

20   The test for personal jurisdiction is generally stated as follows:

21   Where, as here, no federal statute authorizes personal jurisdiction,
         the district court applies the law of the state in which the court sits.
22   California's long-arm statute, Cal. Civ. Proc. Code § 410.10, is
         coextensive with federal due process requirements, so the
23   jurisdictional analyses under state law and federal due process are
         the same. For a court to exercise personal jurisdiction over a
24   nonresident defendant consistent with due process, that defendant
         must have "certain minimum contacts" with the relevant forum
25   "such that the maintenance of the suit does not offend 'traditional
         notions of fair play and substantial justice.'"

26

27   *Mavrix*, 647 F.3d at 1223.

28   There are two categories of personal jurisdiction: (1) general jurisdiction and (2) specific

1   jurisdiction. *Freestream*, 905 F.3d at 602. Plaintiffs contend that the Court has general

2   jurisdiction (and, in the alternative, specific jurisdiction) over Shopify USA and specific

3   jurisdiction over Shopify, Inc. and Ledger.

4   As explained below, the Court lacks general jurisdiction (and specific jurisdiction) over

5   Shopify USA, and lacks specific jurisdiction over Shopify, Inc. and Ledger.

6   1.   The Court Lacks General Jurisdiction Over Shopify USA

7   Where there is general jurisdiction over a defendant, the plaintiff can bring any claim

8   against the defendant in the forum state. Thus, in order for general jurisdiction to obtain, the

9   defendant's contacts with the forum state must be so continuous and systematic as to render the

10   defendant essentially at home in the forum State. *See Daimler AG v. Bauman*, 571 U.S. 117, 122,

11   128 (2014); *see also Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 807 (9th Cir.

12   2004) (asking whether the defendant has continuous and systematic contacts that approximate

13   physical presence in the forum state). "With respect to a corporation, the place of incorporation

14   and principal place of business are 'paradig[m] ... bases for general jurisdiction.'" *Daimler*, 571

15   U.S. at 137. General jurisdiction outside of those forums is available "[o]nly in an exceptional

16   case," *Martinez v. Aero Caribbean*, 764 F.3d 1062, 1070 (9th Cir. 2014), where the defendant's

17   contacts are so "continuous and systematic" as to "'approximate physical presence' in the forum

18   state," *Pestmaster Franchise Network, Inc. v. Mata*, 2017 WL 1956927, at *2 (N.D. Cal. 2017)

19   (quoting *Mavrix*, 647 F.3d at 1223-24).

20   Here, Plaintiffs argue that the Court has general jurisdiction over Shopify USA, but

21   concede that Shopify USA is neither incorporated in California (it is a Delaware corporation), nor

22   is California Shopify USA's principal place of business (Shopify USA's principal place of

23   business is Ottawa, Canada). FAC ¶ 24. Instead, to support their contention that the Court has

24   general jurisdiction over Shopify USA, Plaintiffs observe that Shopify USA *previously* listed San

25   Francisco, CA as its principal place of business since 2014, including, allegedly, during the time

26   period that the data breach took place in 2019. Opposition at 11-13. Plaintiffs point to Shopify

27   USA's business registration filings in various states that continued to list San Francisco as its

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.