PURVI G. PATEL (CA SBN 270702)
PPatel@mofo.com
KELSEY HARRISON (CA SBN 328621)
KHarrison@mofo.com
JOVANNA R. BUBAR (CA SBN 329277)
JBubar@mofo.com
MORRISON & FOERSTER LLP
707 Wilshire Boulevard, Suite 6000
Los Angeles, California 90017-3543
Telephone: 213.892.5200
Facsimile: 213.892.5454

MARK DAVID McPHERSON (CA SBN 307951)
MMcPherson@mofo.com
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94101
Telephone: 415.268.7000
Facsimile: 415.268.7522

Attorneys for Specially Appearing
Defendant LEDGER SAS

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

NAEEM SEIRAFI, EDWARD BATON, ANTHONY COMILLA, BRETT DEENEY, and ABRAHAM VILINGER, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

LEDGER SAS, SHOPIFY (USA) INC., and SHOPIFY INC.,

Defendants.

Case No. 3:21-cv-02470-EMC

DEFENDANT LEDGER SAS's NOTICE OF MOTION AND MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED CLASS ACTION COMPLAINT

Judge: Hon. Edward M. Chen
Date: October 21, 2021
Time: 1:30pm
Courtroom: 5

Complaint filed: April 6, 2021
FAC filed: June 9, 2021
Trial date: none

NOTICE OF MOTION AND MOTION

TO PLAINTIFFS AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on October 21, 2021, at 1:30 p.m., or as soon thereafter as the matter may be heard, in Courtroom 5 of this Court, located at 450 Golden Gate Avenue, San Francisco, California 94102, Defendant Ledger SAS will and hereby does move this Court for an order dismissing Plaintiffs' First Amended Complaint in its entirety or, in the alternative, striking Plaintiffs' overbroad class allegations. Ledger moves, pursuant to Federal Rules of Civil Procedure 9(b), 12(b)(1), 12(b)(2), 12(b)(6), 12(f), and 23(d)(1)(D), and the doctrine of *forum non conveniens*, on the grounds that:

(a) the Court lacks personal jurisdiction over Ledger;

(b) the Northern District of California is an improper forum for this lawsuit;

(c) Plaintiffs fail to satisfy basic pleading standards and the heightened pleading standard for claims sounding in fraud;

(d) Plaintiffs fail to state any claim for relief;

(e) Plaintiffs lack standing for injunctive relief and Plaintiff Naeem Seirafi lacks Article III standing; and

(f) Plaintiffs' "consumer" class allegations are facially overbroad.

The motion is based upon this Notice; the accompanying Memorandum of Points and Authorities, and Declarations of Laura Graniou, Sarah Harris-John, Erin McIntomny, and Quentin Ricomard; the pleadings, files, and records in this action; and such additional evidence and arguments as may be presented at the hearing of this motion.

Dated: July 26, 2021

MORRISON & FOERSTER LLP

By: */s/ Purvi G. Patel*
Purvi G. Patel
Attorneys for Specially Appearing Defendant Ledger SAS

TABLE OF CONTENTS

I. INTRODUCTION 1

II. FACTUAL BACKGROUND 2

III. ARGUMENT 3

- A. The Court Lacks Personal Jurisdiction Over Ledger 3
  - 1. Ledger's California contacts are insufficient for general jurisdiction 4
  - 2. Ledger Technologies' California contacts cannot be imputed to Ledger and in any event are insufficient for general jurisdiction 6
  - 3. The Court lacks specific jurisdiction over Ledger 7
- B. Plaintiffs Agreed to Multiple Forum Selection Clauses, Which Compel Dismissal of Their Claims 11
  - 1. Plaintiffs' claims are within the forum selection clauses 12
  - 2. The forum selection clauses are enforceable 13
  - 3. The public interest factors weigh in favor of enforcing the forum selection clause and dismissing the case 16
  - 4. Even without considering the forum selection clauses, Plaintiffs' claims should be dismissed on *forum non conveniens* grounds 17
- C. The FAC Fails to State a Claim 18
  - 1. Plaintiffs' UCL and CLRA claims, which sound in fraud, fail 19
  - 2. Plaintiffs fail to state a claim for deceit by concealment 24
  - 3. Plaintiffs fail to state a claim for negligence and negligence per se 25
  - 4. Plaintiff Baton's Georgia Fair Business Practices Act and Uniform Deceptive Trade Practices Act claims fail 28
  - 5. Plaintiff Comilla's New York GBL §§ 349 and 350 claims fail 30
  - 6. Plaintiffs' requests for equitable relief must be dismissed because they do not allege they lack an adequate remedy at law 31
  - 7. Declaratory judgement and injunctive relief are not causes of action 33
- D. Plaintiffs Do Not Have Standing to Pursue Injunctive Relief and Plaintiff Seirafi Lacks Standing to Pursue Any Claim 33
  - 1. Plaintiffs lack standing to seek injunctive relief 34
  - 2. Plaintiff Seirafi lacks Article III standing 35
- E. The Court Should Strike Plaintiffs' "Consumer" Class and Subclasses 38

IV. CONCLUSION 40

TABLE OF AUTHORITIES

Page(s)

Cases

Abdale v. N. Shore-Long Island Jewish Health Sys., Inc.,
19 N.Y.S.3d 850 (N.Y. Sup. Ct. 2015) 31

Adobe Sys. Inc. v. Cardinal Camera & Video Ctr., Inc.,
No. 15-cv-02991-JST,
2015 WL 5834135 (N.D. Cal. Oct. 7, 2015) 8, 9

Alexandria Real Estate Equities, Inc. v. Runlabs (UK) Ltd.,
No. 18-CV-07517-LHK,
2019 WL 4221590 (N.D. Cal. Sept. 5, 2019) 8

Amoco Egypt Oil Co. v. Leonis Nav. Co., Inc.,
1 F.3d 848 (9th Cir. 1993) 11

Anderson v. Kimpton Hotel & Rest. Grp., LLC,
No. 19-cv-01860-MMC,
2019 WL 3753308 (N.D. Cal. Aug. 8, 2019) 27

In re Anthem, Inc. Data Breach Litig.,
No. 15-MD-02617-LHK,
2016 WL 3029783 (N.D. Cal. May 27, 2016) 22

Antman v. Uber Techs., Inc.,
No. 15-cv-01175-LB,
2018 WL 2151231 (N.D. Cal. May 10, 2018) 36

In re Arby's Rest. Grp. Inc. Litig.,
No. 1:17-cv-0514-AT,
2018 WL 2128441 (N.D. Ga. Mar. 5, 2018) 29

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 18, 27

Atl. Marine Const. Co. v. U.S. Dist. Ct. for W. Dist. of Texas,
571 U.S. 49 (2013) 11, 17

Baltazar v. Apple, Inc.,
No. CV-10-3231-JF,
2011 WL 588209 (N.D. Cal. Feb. 10, 2011) 22

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007) 18

Bem v. Stryker Corp.,
No. C 15-2485 MMC,
2015 WL 4573204 (N.D. Cal. July 29, 2015)....27

BNSF Ry. Co. v. Tyrrell,
137 S. Ct. 1549 (2017)....5

Bristol-Myers Squibb Co. v. Superior Court,
137 S. Ct. 1773 (2017)....4

Brooks v. Sotheby's,
No. 13-cv-02183 RS,
2013 WL 3339356 (N.D. Cal. July 1, 2013)....16

Butcher's Union Local No. 498 v. SDC Inv., Inc.,
788 F.2d 535 (9th Cir. 1986)....5

Byung Ho Cheoun v. Infinite Energy, Inc.,
363 F. App'x 691 (11th Cir. 2010)....30

Caces-Tiamson v. Equifax,
No. 20-CV-00387-EMC,
2020 WL 1322889 (N.D. Cal. Mar. 20, 2020)....5, 7, 9, 10

Cairo, Inc. v. Crossmedia Services, Inc.,
No. C 04-04825 JW,
2005 WL 756610 (N.D. Cal. Apr. 1, 2005)....15

Carijano v. Occidental Petroleum Corp.,
643 F.3d 1216 (9th Cir. 2011)....17

CE Distribution, LLC v. New Sensor Corp.,
380 F.3d 1107 (9th Cir. 2004)....11

Chandler v. State Farm Mut. Auto. Ins. Co.,
598 F.3d 1115 (9th Cir. 2010)....34

Chowning v. Kohl's Dep't Stores, Inc.,
No. CV 15-08673 RGK,
2016 WL 1072129 (C.D. Cal. Mar. 15, 2016)....32

Clapper v. Amnesty Int'l USA 1138,
133 S. Ct. (2013)....35, 38

CollegeSource, Inc. v. AcademyOne, Inc.,
653 F.3d 1066 (9th Cir. 2011)....4

Collins v. Athens Orthopedic Clinic,
356 Ga. App. 776 (2020)....29, 30, 35

Color Switch LLC v. Fortafy Games DMCC,
377 F. Supp. 3d 1075 (E.D. Cal. 2019)....13, 17

Countrywide Home Loans, Inc., v. Mortg. Guar. Ins. Corp.,
642 F.3d 849 (9th Cir. 2011)....33

Creative Tech. Ltd. v. Aztech Sys. PTE, Ltd.,
61 F.3d 696 (9th Cir. 1995)....17

Czuchaj v. Conair Corp.,
No. 13-CV-1901-BEN (RBB),
2014 WL 1664235 (S.D. Cal. Apr. 18, 2014)....25

DaimlerAG v. Bauman,
571 U.S. 117 (2014)....4, 5, 6

Dent v. Nat'l Football League,
968 F.3d 1126 (9th Cir. 2020)....26

Dewi v. Wells Fargo Bank,
No. CV 12-2891 ABC,
2012 WL 10423239 (C.D. Cal. Aug. 8, 2012)....37

Doe v. Unocal Corp.,
248 F.3d 915 (9th Cir. 2001)....4

Dugas v. Starwood Hotels & Resorts Worldwide, Inc.,
No. 3:16-cv-00014-GPC-BLM,
2016 WL 6523428 (S.D. Cal. Nov. 3, 2016)....34

Eclipse Grp. LLP v. Target Corp.,
No. 15cv1411-JLS-BLM,
2016 WL 8395077 (S.D. Cal. May 26, 2016)....4

Elliot v. Cessna Aircraft Co.,
No. 8:20-cv-00378-SBA,
2021 WL 2153820 (C.D. Cal. May 25, 2021)....8

Elofson v. Bivens,
No. 15-cv-05761-BLF,
2017 WL 566323 (N.D. Cal. Feb. 13, 2017)....9

In re Equifax, Inc., Customer Data Sec. Breach Litig.,
362 F. Supp. 3d 1295 (N.D. Ga. 2019)....28

In re Facebook, Inc., Consumer Priv. User Profile Litig.,
402 F. Supp. 3d 767 (N.D. Cal. 2019)....24

Fink v. Time Warner Cable,
714 F.3d 739 (2d Cir. 2013) 30

Flores-Mendez v. Zoosk, Inc.,
No. C 20-04929 WHA,
2021 WL 308543 (N.D. Cal. Jan. 30, 2021) 23

Guaranty Trust Co. of New York v. York,
326 U.S. 99 (1945) 32

Gest v. Bradbury,
443 F.3d 1177 (9th Cir. 2006) 34, 35

Grisham v. Philip Morris, Inc.,
670 F. Supp. 2d 1014 (C.D. Cal. 2009) 24

Haskins v. Symantec Corp.,
No. 13-cv-01834-JST,
2013 WL 6234610 (N.D. Cal. Dec. 2, 2013) 21

Hovsepian v. Apple, Inc.,
No. 08-5788 JF (PVT),
2009 WL 5069144 (N.D. Cal. Dec. 17, 2009) 39

HSM Holdings, LLC v. Mantu I.M. Mobile Ltd.,
No. 19-cv-04391-JST,
2020 WL 7220462 (N.D. Cal. Jan. 30, 2020) 12

Hudson-munoz, LLC v. U.S. Waffle Co., Inc.,
No. 2:19-cv-01960-ODW,
2019 WL 3548919 (C.D. Cal. Aug. 5, 2019) 10

Imageline, Inc. v. Hendricks,
No. CV 09-1870 DSF,
2009 WL 10286181 (C.D. Cal. Aug. 12, 2009) 9

Int'l Shoe Co. v. Washington,
326 U.S. 310 (1945) 4

Jackson v. Loews Hotels, Inc.,
No. ED CV 18-827-DMG,
2019 WL 6721637 (C.D. Cal. July 24, 2019) 37

Kearns v. Ford Motor Co.,
567 F.3d 1120 (9th Cir. 2009) 19

Khoja v. Orexigen Therapeutics, Inc.,
899 F.3d 988 (9th Cir. 2018) 14

Krottner v. Starbucks Corp.,
628 F.3d 1139 (9th Cir. 2010)....................34

Kuhns v. Scottrade, Inc.,
868 F.3d 711 (8th Cir. 2017)....................27

Kwikset Corp. v. Superior Court,
51 Cal. 4th 310 (2011) 22

LaCross v. Knight Transportation, Inc.,
95 F. Supp. 3d 1199 (C.D. Cal. 2015)....................15

Lavie v. Procter & Gamble Co.,
105 Cal. App. 4th 496 (2003)....................19

Lightfoot v. MoneyonMobile, Inc.,
No. 18-CV-07123-YGR,
2019 WL 2476624 (N.D. Cal. June 13, 2019) 16

Livingston v. Pneu-Logic Corp.,
No. 20-cv-07155-JCS,
2021 WL 1375903 (N.D. Cal. Apr. 12, 2021) 11

Low v. LinkedIn Corp.,
No. 11-CV-01468-LHK,
2011 WL 5509848 (N.D. Cal. Nov. 11, 2011)....................36

Lueck v. Sundstrand Corp.,
236 F.3d 1137 (9th Cir. 2001)....................17, 18

Lujan v. Defs. of Wildlife,
504 U.S. 555 (1992)....................34, 36

In re MacBook Keyboard Litig.,
No. 5:18-cv-02813-EJD,
2020 WL 6047253 (N.D. Cal. Oct. 13, 2020)....................32, 33

Matus v. Premium Nutraceuticals, LLC,
No. EDCV 15-01851 DDP (DTBx),
2016 WL 3078745 (C.D. Cal. May 31, 2016) 7

Maurizio v. Goldsmith,
230 F.3d 518 (2d Cir. 2000)....................30

Mavrix Photo, Inc. v. Brand Techs., Inc.,
647 F.3d 1218 (9th Cir. 2011)....................4

Mazza v. Am. Honda Motor Co.,
666 F.3d 581 (9th Cir. 2012)....................39

Mazzola v. Roomster Corp.,
No. CV 10-5954 AHM,
2010 WL 4916610 (C.D. Cal. Nov. 30, 2010)....................16

McGlinchy v. Shell Chem. Co.,
845 F.2d 802 (9th Cir. 1988)....................18

Meier v. Midwest Recreational Clearinghouse, LLC,
No. 2:10-cv-01026-MCE-GGH,
2010 WL 2738921 (E.D. Cal. July 12, 2010)....................15

Mendoza v. City of Los Angeles,
66 Cal. App. 4th 1333 (1998)....................27

Meyer v. Sprint Spectrum L.P.,
45 Cal. 4th 634 (2009)....................23

MGA Ent. Inc. v. Deutsche Bank AG,
No. CV 11-4932 GW (RZX),
2012 WL 12892902 (C.D. Cal. Feb. 27, 2012)....................16, 17

Mocha Mill, Inc. v. Port of Mokha, Inc.,
No. 18-cv-02539-HSG,
2019 WL 1048252 (N.D. Cal. Mar. 5, 2019)....................10

Moore-Davis Motors, Inc. v. Joyner,
252 Ga. App. 617 (2001)....................29

Moretti v. Hertz Corp.,
No. C 13-02972 JSW,
2014 WL 1410432 (N.D. Cal. Apr. 11, 2014)....................17

Morrill v. Scott Fin. Corp.,
873 F.3d 1136 (9th Cir. 2017)....................7

Novak v. United States,
795 F.3d 1012 (9th Cir. 2015)....................37

In re NVIDIA Corp. Sec. Litig.,
768 F.3d 1046 (9th Cir. 2014)....................14, 21

O'Keefe v. Inca Floats, Inc.,
No. C-97-1225 VRW,
1997 WL 703784 (N.D. Cal. 1997)....................27

Oneto v. Ryland Grp., Inc.,
No. EDCV 09-01670 VAP (DTBx),
2010 WL 11506425 (C.D. Cal. Mar. 31, 2010)....................37

Orlander v. Staples, Inc.,
802 F.3d 289 (2d Cir. 2015)........30

Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A.,
85 N.Y.2d 20 (1995)........31

Owens v. Wells Fargo Bank, N.A.,
No. C 09-3354 PJH,
2009 WL 3353313 (N.D. Cal. 2009)........33

In re Packaged Seafood Prod. Antitrust Litig.,
338 F. Supp. 3d 1118 (S.D. Cal. 2018)........6

Panavision Int'l, L.P. v. Toeppen,
141 F.3d 1316 (9th Cir. 1998)........4

Peterson v. Cellco Partnership,
164 Cal. App. 4th 1583 (2008)........23

Picot v. Weston,
780 F.3d 1206 (9th Cir. 2015)........8

Pirozzi v. Apple Inc.,
913 F. Supp. 2d 840 (N.D. Cal. 2012)........22

Quiroz v. Seventh Ave. Ctr.,
140 Cal. App. 4th 1256 (2006)........26

Rahman v. Marriott Int'l, Inc.,
No. SA CV 20-00654-DOC-KES,
2021 WL 346421 (C.D. Cal. Jan. 12, 2021)........35

Ranza v. Nike, Inc.,
793 F.3d 1059 (9th Cir. 2015)........4, 5, 6

Razuki v. Caliber Home Loans, Inc.,
No. 17cv1718-LAB (WVG),
2018 WL 6018361 (S.D. Cal. Nov. 15, 2018)........27

Ruelas Aldaba v. Michelin North America, Inc.,
No. C 04–5369 MHP,
2005 WL 3560587 (N.D. Cal. Dec. 29, 2005)........18

Ruiz v. Gap, Inc.,
540 F. Supp. 2d 1121 (N.D. Cal. 2008)........23

Sabre Int'l Sec. v. Torres Advanced Enter. Sols., LLC,
60 F. Supp. 3d 21 (D.D.C. 2014)........6

Sanders v. Apple Inc.,
672 F. Supp. 2d 978 (N.D. Cal. 2009) 40

Sandoval v. Ali,
34 F. Supp. 3d 1031 (N.D. Cal. 2014) 39

Sateriale v. R.J. Reynolds Tobacco Co.,
697 F.3d 777 (9th Cir. 2012)....................21

Sawyer v. Bill Me Later, Inc.,
No. CV 10-04461 SJO,
2010 WL 5289537 (C.D. Cal. Oct. 4, 2010) 15

Schwarzenegger v. Fred Martin Motor Co.,
374 F.3d 797 (9th Cir. 2004)....................7, 9, 10

Scott v. Jayco, Inc.,
No. 1:18-cv-00861-LJO-JLT,
2018 WL 5816153 (E.D. Cal. Nov. 5, 2018) 15

Sion v. SunRun, Inc.,
No. 16-cv-05834-JST,
2017 WL 952953 (N.D. Cal. Mar. 13, 2017) 37

In re Sling Media Slingbox Advert. Litig.,
202 F. Supp. 3d 352 (S.D.N.Y. 2016)....................31

Sonner v. Premier Nutrition Corp.,
971 F.3d 834 (9th Cir. 2020).................... xiv, 31, 32, 33

In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,
903 F. Supp. 2d 942 (S.D. Cal. 20112) 19, 20, 23, 25

Spokeo, Inc. v. Robins,
136 S. Ct. 1540 (2016) 34

Stack v. Progressive Select Ins. Co.,
No. 20-cv-00338-LB,
2020 WL 5517300 (N.D. Cal. Sept. 14, 2020) 4

*Tae Youn Shim v. Lawle*r,
No. 17-CV-04920-EMC,
2019 WL 2996443 (N.D. Cal. July 9, 2019) 24

Tellabs, Inc. v. Makor Issues & Rights, Ltd.,
551 U.S. 308 (2007) 14

Terpin v. AT&T Mobility, LLC,
No. 2:18-cv-06975-ODW,
2020 WL 5369410 (C.D. Cal. Sept. 8, 2020)....24

Terrill v. Electrolux Home Prod., Inc.,
753 F. Supp. 2d 1272 (S.D. Ga. 2010)....29

Thomas v. Facebook,
No. 1:18-cv-00856-LJO-BAM,
2018 WL 3915585 (E.D. Cal. Aug. 15, 2018)....15

Tiismann v. Linda Martin Homes Corp.,
281 Ga. 137 (2006)....29

Vess v. Ciba-Geigy Corp. USA,
317 F.3d 1097 (9th Cir. 2003)....19, 20

Voodoo SAS v. SayGames LLC,
No. 19-cv-07480-BLF,
2020 WL 3791657 (N.D. Cal. July 7, 2020)....8

Walden v. Fiore,
571 U.S. 277 (2014)....10

Warth v. Seldin,
422 U.S. 490 (1975)....34, 36

Willingham v. Glob. Payments, Inc.,
No. 1:12-CV-01157-RWS,
2013 WL 440702 (N.D. Ga. Feb. 5, 2013)....26, 35

Wishnev v. Nw. Mut. Life Ins. Co.,
162 F. Supp. 3d 930 (N.D. Cal. 2016)....33

In re Yahoo! Inc. Customer Data Sec. Breach Litig.,
No. 16-MD-02752-LHK,
2017 WL 3727318 (N.D. Cal. Aug. 30, 2017)....22

Yei A. Sun v. Advanced China Healthcare, Inc.,
901 F.3d 1081 (9th Cir. 2018)....12, 13

In re Zappos.com, Inc.,
888 F.3d 1020 (9th Cir. 2018)....35

In re Zappos.com, Inc. Customer Data Sec. Breach Litig.,
108 F. Supp. 3d 949 (D. Nev. 2015)....35, 37

Statutes

Cal. Bus. & Prof. Code § 17200, *et seq.* 3

Cal. Bus. & Prof. Code § 17203 32

Cal. Bus. & Prof. Code § 17204 22

Cal. Bus. & Prof. Code § 17208 5

Cal. Civ. Code § 1709 ....3, 24

Cal. Civ. Code § 1710 ....3, 24

Cal. Civ. Code § 1750, *et seq.* 3

Cal. Civ. Code § 1780(a) 23

Cal. Civ. Code § 1798.82 36

Cal. Evid. Code § 669(a) 26

Georgia Fair Business Practices Act, O.C.G.A. 10-1-393, *et seq.* .... xiv, 3, 28

Georgia Uniform Deceptive Trade Practices Act, O.C.G.A. 10-1-370, *et seq.* .... xiii, 3

New York Deceptive Trade Practices Act, N.Y. Gen. Bus. Law § 340, *et seq.* .... xiii, 3

New York General Business Law § 349 .... *passim*

New York General Business Law § 350 .... *passim*

Other Authorities

Fed. R. Civ. Proc., Rule 9(b) .... i, 19, 22, 24

Fed. R. Civ. Proc., Rule 12(b)(1) .... i, 34

Fed. R. Civ. Proc., Rule 12(b)(2) i

Fed. R. Civ. Proc., Rule 12(b)(6) .... i, 18

Fed. R. Civ. Proc., Rule 12(f) .... i, xii, 39

Fed. R. Civ. Proc., Rule 23(d)(1)(D) .... i, 39

https://support.ledger.com/hc/en-us/articles/360015559320-E-commerce-and-Marketing-data-breach-FAQ?support=true (last visited July 26, 2021) 21

https://shop.ledger.com/pages/privacy-policy (last visited July 26, 2021) 12, 14

https://www.fastpeoplesearch.com/naeem-seirafi_id_G6100017820194900856
(last visited July 26, 2021) 36

STATEMENT OF THE ISSUES TO BE DECIDED

This motion raises the following issues:

1. **Personal Jurisdiction**. Whether this action should be dismissed for lack of personal jurisdiction.

2. ***Forum Non Conveniens***. Whether Plaintiffs' claims should be dismissed pursuant to the doctrine of *forum non conveniens*, because (a) Plaintiffs agreed to forum selection clauses in Ledger's Privacy Policy, the Ledger Sales Terms and Conditions, and/or the Ledger Live Terms of Use, and (b) even without considering those forum selection clauses, this action has no connection with this forum.

3. **UCL and CLRA**. Whether Plaintiffs' claims for violations of the UCL and CLRA should be dismissed because they cannot plausibly plead reliance and Plaintiff Seirafi also does not plausibly plead injury.

4. **Deceit by Concealment.** Whether Plaintiffs' claim for deceit by concealment should be dismissed when they do not allege Ledger had a duty to disclose or concealed any material facts from Plaintiffs.

5. **Negligence and Negligence Per Se**. Whether Plaintiffs' claims for negligence and negligence per se should be dismissed when Plaintiffs do not plead facts showing Ledger breached any duty that proximately caused their alleged injuries and negligence per se is not an independent cause of action.

6. **Georgia Fair Business Practices Act and Uniform Deceptive Trade Practices Act**. Whether Plaintiff Baton's claims under the GFBPA and GUDTPA should be dismissed because there is no statutory duty to safeguard a person's contact information in Georgia, Baton does not allege he relied on any alleged misrepresentations, and he lacks standing to seek injunctive relief.

7. **New York General Business Law Sections 349 and 350.** Whether Plaintiff Comilla's NY GBL claims should be dismissed because he does not allege any materially misleading statements.

8. **Requests for Equitable Relief.** Whether Plaintiffs' requests for equitable relief should be dismissed under *Sonner v. Premier Nutrition Corp.*, because they seek damages and do not allege they lack an adequate remedy at law.

9. **Declaratory Judgment and Injunctive Relief**. Whether Plaintiffs' cause of action for declaratory judgment and injunctive relief should be dismissed because declaratory judgment and injunctive relief are remedies, not independent causes of action.

10. **Standing**. Whether Plaintiffs having standing to seek injunctive relief when an injunction will not redress their alleged injuries and they do not allege any future injury that is certainly impending, and whether Plaintiff Seirafi has Article III standing when he has not alleged an adequate injury.

11. **Rule 12(f) Motion to Strike**. Whether Plaintiffs' overbroad consumer class and subclasses should be stricken as "immaterial" and "impertinent" because they are unrelated to Plaintiffs' theory of the case and by definition include individuals who have not been injured.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Defendant Ledger SAS, a French corporation headquartered in Paris, sells hardware wallets through its e-commerce website, which is run on co-Defendant Shopify Inc.'s platform. The password-protected wallets allow customers to control their cryptocurrency assets. From April to June 2020, Ledger was the victim of two separate security incidents: cyber-criminals stole a "list of Ledger's customers, as well as email addresses and other contact information" (FAC ¶ 8), and separately, "Shopify employees … acquired and exported Ledger's customer transactional records" (*id.* ¶ 78). When Ledger became aware of the incidents, it immediately investigated and informed its customers. Criminals only accessed contact information, including in some instances names, phone numbers, email addresses, and postal addresses.

Plaintiffs—Ledger customers from California, Georgia, New York, the United Kingdom, and Israel—seek to recover from Ledger for the acts of cyber-criminals, after other unnamed criminals allegedly used the information disclosed to target Plaintiffs. Plaintiffs are trying to recover from Ledger for the conduct of at least two sets of criminals, not for anything Ledger itself did or failed to do. Missing from the 276-paragraph First Amended Complaint, however, is any allegation that the security incidents:

- Resulted in the disclosure of Plaintiffs' sensitive personal information, such as their payment card information, account information, or passwords protecting their hardware wallets or crypto assets.
- Implicated in any way the Ledger wallets Plaintiffs purchased. The wallets remain secure; no one but each Plaintiff can access the information stored on each Plaintiff's wallet, and no Plaintiff alleges otherwise.

For these reasons and others, Plaintiffs cannot pursue their claims against Ledger in this Court, and their claims fail as a matter of law wherever they choose to pursue them.

First, this Court lacks personal jurisdiction over Ledger. Plaintiffs cannot allege that Ledger directed any conduct at California. Only one of the five plaintiffs lives in California, and even as to that Plaintiff, there are insufficient contacts for personal jurisdiction. Ledger's sole contact with California is its website—which is accessible globally—from which the California Plaintiff purchased a Ledger hardware wallet.

Second, while Plaintiffs quote heavily from Ledger's website in the FAC, they ignore entirely the terms they agreed to when they purchased Ledger wallets and services and the Privacy Policy to which they agreed by continuing to use Ledger's services. Plaintiffs' claims fall within the scope of forum selection clauses contained in Ledger's Privacy Policy, the Sales Terms and Conditions, and the Ledger Live Terms of Use, mandating that their claims against Ledger be resolved in France. Plaintiffs' claims should therefore be dismissed under the *forum non conveniens* doctrine, including because even absent those forum selection clauses, this action has no connection with the Northern District of California.

Third, Plaintiffs have not sufficiently pled violations of the various statutory and common law claims they assert, and all of those claims should be dismissed. The Court should also dismiss Plaintiffs' requests for equitable relief because they admit that they have adequate remedies at law. Plaintiffs also lack standing to seek injunctive relief, and Plaintiff Naeem Seirafi lacks Article III standing to bring any claims.

Finally, the Court should strike Plaintiffs' proposed "consumer" class and subclasses, as they are facially overbroad. The classes are unrelated to the theory of Plaintiffs' case and by definition include individuals who have not been injured.

For these reasons and those set forth below, the Court should dismiss the First Amended Complaint as against Ledger.

II. FACTUAL BACKGROUND

Ledger is a French company with its principal place of business in Paris, France. (FAC ¶ 21; Declaration of Quentin Ricomard in support of Ledger's Motion to Dismiss ("Ricomard Decl.") ¶ 6.) It sells hardware wallets—the Ledger Nano X and Ledger Nano S—through its e-commerce website, which operates on Shopify Inc.'s platform. (FAC ¶¶ 2, 16-17, 74; Ricomard Decl. ¶ 4.) The password-protected hardware wallets store a customer's private keys, which allow customers to manage their cryptocurrency. (FAC ¶ 2.) Plaintiffs allege they each bought a Ledger Nano X and/or Nano S through Ledger's e-commerce platform between July 2017 and June 2020. (*Id.* ¶¶ 16-20.) Plaintiffs allege they provided their names, email addresses, telephone numbers, and postal addresses. (*Id.*) When Plaintiffs purchased the hardware wallets and through their continued use of the wallets and Ledger's services, they each agreed to Ledger's Privacy Policy, the Ledger Sales Terms and Conditions, and the Ledger Live Terms of Use, all of which contain forum selection clauses compelling Plaintiffs to litigate their claims in France. (Declaration of Laura Graniou in support of Ledger's Motion to Dismiss ("Graniou Decl.") ¶¶ 3-8, Ex. A at 13, Ex. B at 23, Ex. C at 41.)

Plaintiffs' claims arise out of two security incidents involving Plaintiffs' contact information. (FAC ¶¶ 78, 79, 88.) Plaintiffs allege that between April and June 2020, rogue Shopify "employees" exported Ledger's customer transactional records (the "Shopify incident"). (*Id.* ¶¶ 78-79.) They allege Shopify publicly announced the theft on September 22, 2020, but did not notify Ledger that its customers were affected until December 23, 2020. (*Id.* ¶¶ 79, 82, n. 8.) Plaintiffs also allege that an unauthorized third party gained access to Ledger's e-commerce database through an application programming interface ("API") key on June 25, 2020 (the "Ledger cyber attack"). (*Id.* ¶ 88.) They assert Ledger informed them of the Ledger cyber attack two weeks after it occurred. (*Id.*)

Plaintiffs do not and cannot allege that the cyber criminals infiltrated the security of a single hardware wallet or that either incident affected the security of their hardware wallet. Despite this, Plaintiffs assert nine claims[1] on behalf of a purported class of all persons residing in the United States, the United Kingdom, or Israel who purchased a hardware wallet from Ledger or an authorized reseller—including those persons whose information was ***not disclosed*** in either the Shopify incident or the Ledger cyber attack. (*Id.* ¶ 145.)

III. ARGUMENT

A. The Court Lacks Personal Jurisdiction Over Ledger

When a nonresident defendant like Ledger challenges personal jurisdiction, Plaintiffs bear the burden of proof to demonstrate that the Court properly may exercise jurisdiction. *Doe v. Unocal Corp.*, 248 F.3d 915, 922 (9th Cir. 2001). "[A] Rule 12(b)(2) challenge to personal jurisdiction may attack the legal theory supporting jurisdiction based on the facts as pleaded (a facial attack) or the facts themselves (a factual attack)." *Eclipse Grp. LLP v. Target Corp.*, No. 15cv1411-JLS-BLM, 2016 WL 8395077, at *7 (S.D. Cal. May 26, 2016). The Court "may consider declarations and other evidence outside the pleadings in determining whether it has personal jurisdiction." *Stack v. Progressive Select Ins. Co.*, No. 20-cv-00338-LB, 2020 WL 5517300, at *4 (N.D. Cal. Sept. 14, 2020) (citing *Unocal Corp.*, 248 F.3d at 922). The Court "may not assume the truth of [the complaint's] allegations . . . which are contradicted by" a declaration. *Mavrix Photo, Inc. v. Brand Techs., Inc.*, 647 F.3d 1218, 1223 (9th Cir. 2011).

---

[1] The claims are for: (1) negligence; (2) negligence per se; (3) declaratory judgment and injunctive relief; (4) violation of California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*; (5) violation of the California Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code § 1750, *et seq.*; (6) deceit by concealment, Cal. Civ. Code §§ 1709, 1710; (7) violation of the Georgia Uniform Deceptive Trade Practices Act, O.C.G.A. 10-1-370, *et seq.*; (8) violation of the Georgia Fair Business Practices Act, O.C.G.A. 10-1-393, *et seq.*; and (9) violation of the New York Deceptive Trade Practices Act, N.Y. Gen. Bus. Law § 340, *et seq.*

A district court must apply the personal jurisdiction rules of the forum state. *CollegeSource, Inc. v. AcademyOne, Inc.*, 653 F.3d 1066 (9th Cir. 2011). California's "long-arm" statute is coextensive with federal due process, and thus the jurisdictional analysis under state law and federal due process are the same. *See Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1320 (9th Cir. 1998). Constitutional due process concerns are satisfied when a nonresident defendant has "certain minimum contacts with [the forum state] such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice." *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945) (internal quotation marks and citation omitted). Applying the "minimum contacts" analysis, there are two potential bases for jurisdiction: general and specific. *See Bristol-Myers Squibb Co. v. Superior Court*, 137 S. Ct. 1773, 1779-80 (2017). Neither is present here.

1. Ledger's California contacts are insufficient for general jurisdiction

Absent "exceptional" circumstances, general jurisdiction exists over a corporate defendant only in its state of incorporation and principal place of business. *DaimlerAG v. Bauman*, 571 U.S. 117, 138-39, 139 n.19 (2014). A plaintiff seeking to invoke general jurisdiction over a non-resident defendant must establish that the defendant's contacts with the forum state are "so constant and pervasive as to render [it] essentially at home in" that state. *Id.* at 122 (internal citation and quotation marks omitted). This is an "exacting standard." *See Ranza v. Nike, Inc.*, 793 F.3d 1059, 1069 (9th Cir. 2015) (quoting *CollegeSource, Inc.*, 653 F.3d at 1074).

Ledger is incorporated and has its principal place of business in Paris, France. (Ricomard Decl. ¶ 6.) Thus, to establish general jurisdiction over Ledger Plaintiffs must allege facts making it plausible that Ledger's contacts with California are "so constant and pervasive as to render it essentially at home in" California. *Daimler*, 571 U.S. at 122. Plaintiffs fail to do so. The only allegations Plaintiffs make as to Ledger's direct contacts with California are that it has "substantial contacts" with and "receives substantial benefits" from California, does "business in the State of California," sells its hardware wallets on an "online international marketplace, including . . . California," and has an office in San Francisco. (FAC ¶¶ 21, 26.) These vague and conclusory allegations are incorrect and would be insufficient to establish general jurisdiction even if they were true.[2]

Ledger does not have any offices in California (or anywhere else in the United States). (Ricomard Decl. ¶ 7.) It does not have any employees or officers located in the United States (all of its employees and corporate officers are located in France and, to a lesser extent, Switzerland). (*Id.*) Its corporate records are not located in California, it is not registered to do business in California, and it has no agent for service of process in California. (*Id.* ¶¶ 8-9.) Since April 2017, only approximately 7.03% of Ledger's total hardware wallet revenue is from California (Ledger's hardware wallet revenue from the United States as a whole during this time period is only about 35.83%).[3] (*Id.* ¶ 10.) These limited contacts with California are not nearly enough to subject Ledger to general jurisdiction in the State. *See BNSF Ry. Co. v. Tyrrell*, 137 S. Ct. 1549, 1554, 1559 (2017) (no general jurisdiction where defendant had over 2,000 employees and 2,000 miles of railroad track in the forum state, generated revenue in the forum state, and maintained a facility in the forum state); *Ranza*, 793 F.3d at 1069 (no general jurisdiction where defendant had 20 employees working in Oregon, entered into contracts whereby Nike in Oregon was to act as the defendant's agent in various business arrangements, and sold its products in Oregon stores).

---

[2] "[N]onspecific conclusory statement[s are] not enough" to establish personal jurisdiction. *Butcher's Union Local No. 498 v. SDC Inv., Inc.*, 788 F.2d 535, 540 (9th Cir. 1986). Moreover, "'doing business' has long been abandoned as the test for general jurisdiction." *Ranza*, 793 F.3d at 1070; *see also Caces-Tiamson v. Equifax*, No. 20-CV-00387-EMC, 2020 WL 1322889, at *2 (N.D. Cal. Mar. 20, 2020) (noting the Supreme Court has "rejected the proposition that there is general jurisdiction over a corporation in every in every State in which a corporation engages in a substantial, continuous, and systematic course of business").

[3] The longest possible applicable statutory period here is four years. *See* Cal. Bus. & Prof. Code § 17208 (providing four-year limitations period for UCL claims).

2. Ledger Technologies' California contacts cannot be imputed to Ledger and in any event are insufficient for general jurisdiction

Plaintiffs cannot establish general jurisdiction over Ledger based on the contacts of its subsidiary, Ledger Technologies. (FAC ¶¶ 22, 28-29.) In *Daimler*, the Supreme Court rejected such an attempt to subject a foreign corporation to general jurisdiction based on the contacts of its United States subsidiary. 571 U.S. at 136. Imputing a domestic entity's contacts to its foreign affiliate for jurisdictional purposes is permissible only if there is "an alter ego relationship between the entities." *Ranza*, 793 F.3d at 1071, 1079. That "extreme" theory requires "deviating from the rule of corporate separateness" and should be "sparingly used." *In re Packaged Seafood Prod. Antitrust Litig.*, 338 F. Supp. 3d 1118, 1147 (S.D. Cal. 2018).

Here, Plaintiffs' allegations that Ledger Technologies operates as Ledger's alter ego are far too bare and conclusory to satisfy the standard for ignoring the corporate separation between them.[4] Even if an alter ego relationship existed between Ledger and Ledger Technologies, Ledger Technologies does not have sufficient contacts with California to establish general jurisdiction over it or Ledger. *See In re Packaged Seafood Prod. Antitrust Litig.*, 338 F. Supp. 3d at 1143 (no basis to subject parent to general jurisdiction where combined contacts are not sufficient to render parent at home in the forum). Ledger Technologies is incorporated in Delaware and its principal place of business is in Paris, France, where the majority of its corporate officers are located.[5] (Ricomard Decl. ¶ 16.) Its sole United States office is in New

---

[4] Nor could Plaintiffs prove alter ago, as the two entities are separate corporations with different business lines. (Ricomard Decl. ¶¶ 3, 13.) Their businesses and their corporate books and records are separately maintained. (*Id.* ¶ 2.)

[5] Plaintiffs are correct that Ledger Technologies previously had an office in San Francisco, California (FAC ¶ 22, 28), but the existence of a single office in the forum state is insufficient for general jurisdiction. *See Daimler*, 571 U.S. at 123, 139 (defendant not "at home" in California for general jurisdiction purposes, even with its subsidiary's contacts imputed to it, including that it maintained at least three California facilities in the State.) Regardless, general jurisdiction is determined no earlier than at the time the complaint is filed. *Sabre Int'l Sec. v. Torres Advanced Enter. Sols., LLC*, 60 F. Supp. 3d 21, 30 (D.D.C. 2014) (collecting cases).

York, New York, where its bank account is maintained. (*Id.* ¶¶ 17, 18.) Ledger Technologies does not have any employees or officers in California, and its only United States employees (two) and officer (one) are in New York. (*Id.* ¶ 17.) Ledger Technologies does not rent, lease, own, or otherwise possess any real property in California. (*Id.* ¶ 15.) The only contacts Ledger Technologies has in California are a small percentage of its total revenue (approximately 8.1%),[6] a California business registration, and an appointment of an agent for service of process. (*Id.* ¶ 14.) These limited contacts cannot subject Ledger Technologies to general jurisdiction in the State, and therefore cannot be used to subject Ledger to general jurisdiction in the State, either. *See supra* at p. 5-6 (citing *See BNSF Ry. Co.* and *Ranza*).

3. The Court lacks specific jurisdiction over Ledger

Specific jurisdiction exists where: (1) the defendant "purposefully directed" its activities towards California; (2) the plaintiff's claims "arise out of" those forum-related activities; and (3) the exercise of jurisdiction is "reasonable." *See Morrill v. Scott Fin. Corp.*, 873 F.3d 1136, 1142 (9th Cir. 2017). "The plaintiff bears the burden of satisfying the first two prongs of the test." *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004). Plaintiffs cannot meet this burden here.

a. Ledger did not purposefully direct its activities towards California

The purposeful direction test applies where, as here, Plaintiffs assert primarily tort or statutory claims. *See, e.g., Schwarzenegger*, 374 F.3d at 802; *Caces-Tiamson*, 2020 WL 1322889, at *3 (courts should apply a purposeful direction analysis to tort claims arising from data breaches); *Matus v. Premium Nutraceuticals, LLC*, No. EDCV 15-01851 DDP (DTBx), 2016 WL 3078745, at *3 (C.D. Cal. May 31, 2016) (applying purposeful direction test where the plaintiff alleged violations of the UCL, FAL, and CLRA and a claim for negligent misrepresentation). A defendant "purposefully direct[s]" [its] activities at the forum if [it]: (1) committed an intentional act, (2) expressly aimed at the forum state, (3) causing harm that the defendant knows is likely to be suffered in the forum state." *Picot v. Weston*, 780 F.3d 1206, 1214 (9th Cir. 2015) (internal quotations and citation omitted); *see also Voodoo SAS v. SayGames LLC*, No. 19-cv-07480-BLF, 2020 WL 3791657, at *3 (N.D. Cal. July 7, 2020). "Failing to sufficiently plead any one of these three elements … is fatal to Plaintiff[s'] attempt to show personal jurisdiction." *Alexandria Real Estate Equities, Inc. v. Runlabs (UK) Ltd.*, No. 18-CV-07517-LHK, 2019 WL 4221590, at *7 (N.D. Cal. Sept. 5, 2019) (internal quotations omitted).

---

[6] Ledger Technologies sells Ledger Vault, a SaaS (software as a service) solution for securing crypto-assets throughout the United States, to corporate and institutional customers; it is not a product available to individual customers. (Ricomard Decl. ¶ 13.)

While Ledger may have committed an "intentional act" by offering hardware wallets for sale on its internationally accessible website, it did not expressly aim any act at California and did not cause harm that Ledger knew was likely to be suffered in California (if it caused any harm at all). "Operating a universally accessible website alone is generally insufficient to satisfy the express aiming requirement." *Elliot v. Cessna Aircraft Co.*, No. 8:20-cv-00378-SBA (DSx), 2021 WL 2153820, at *3 (C.D. Cal. May 25, 2021) ("the fact that Defendant maintains an interactive website that reaches potential customers in California does not establish specific jurisdiction"); *see also Adobe Sys. Inc. v. Cardinal Camera & Video Ctr., Inc.*, No. 15-cv-02991-JST, 2015 WL 5834135, at *5 (N.D. Cal. Oct. 7, 2015) ("not all material placed on the Internet is, solely by virtue of its universal accessibility, expressly aimed at every state in which it is accessed"). "A defendant is required to do 'something more'—namely, the defendant must engage in conduct directly targeting the forum, such as to display content or advertisements that appeal to, and profit from, an audience in a particular state." *Elliot*, 2021 WL 2153820, at *3.

Here, beyond conclusory allegations that Ledger conducts business in and has "substantial contacts" with California—allegations that Ledger's sworn declaration exposes as baseless—Plaintiffs only allege that Ledger solicits customers in the United States and California.[7] (FAC ¶¶ 21, 26, 32.) Plaintiffs add that Ledger offers hardware wallets for sale "on an online international marketplace" that includes California and that allegedly 33% of the compromised address information belonged to individuals with United States (not California) addresses. (*Id.* ¶¶ 21, 32.) In short, Plaintiffs allege nothing more than the unremarkable fact that Ledger operates a universally accessible website. Plaintiffs do not allege that Ledger aims its business specifically at California, nor could they, as Ledger does not focus its business or advertising on any particular state in the United States, much less California itself. (Ricomard Decl. ¶ 11.) Accordingly, Plaintiffs fail to sufficiently plead the express aiming element. *See Adobe Sys. Inc. v. Cardinal Camera & Video Ctr.*, Inc., No. 15-cv-02991-JST, 2015 WL 5834135, at *5 (N.D. Cal. Oct. 7, 2015) (website not targeted at a particular forum where it "has a broad and indiscriminate scope"); *Imageline, Inc. v. Hendricks*, No. CV 09-1870 DSF (AGRx), 2009 WL 10286181, at *4 (C.D. Cal. Aug. 12, 2009) ("Defendants did not purposefully direct actions towards California" where "they made their goods available on the Internet and those goods happened to have been purchased in California."); *Caces-Tiamson*, 2020 WL 1322889, at *3 (specific jurisdiction cannot be based on the "mere fact" that a defendant "provides services to customers nationwide, including but not limited to California").

---

[7] Plaintiffs also allege that the Court has jurisdiction over Ledger because "Shopify (USA) acted as [Ledger's] agent for the conduct giving rise to Plaintiffs' claims." (FAC ¶ 32.) Plaintiffs, however, do not provide any support for this statement or explain what Shopify (USA)'s actions were, let alone whether those actions took place in California. The allegation is furthermore untrue. Ledger does not have a business relationship with Shopify (USA), Inc.; its contract is with Shopify, Inc. (Declaration of Sarah Harris-John ¶ 6; Declaration of Erin McIntomny ¶ 4.) In any event, for the reasons discussed in Shopify (USA) Inc.'s motion to dismiss, the Court does not have jurisdiction over Shopify (USA) Inc. either.

Plaintiffs also fail to establish that Ledger's act of offering hardware wallets for sale on its universally accessible website caused any harm in California, let alone harm Ledger knew was likely to be suffered there. *See Elofson v. Bivens*, No. 15-cv-05761-BLF, 2017 WL 566323, at *5 (N.D. Cal. Feb. 13, 2017) (plaintiff failed to establish purposeful direction where he did not allege any of the defendant's actions caused him harm). Plaintiffs' inability to show that Ledger purposefully directed any of its activities at California, standing alone, compels dismissal of Plaintiffs' claims for lack of personal jurisdiction. *Schwarzenegger*, 374 F.3d at 802 (if plaintiffs fail to establish that defendant purposefully directed activities at the forum state *or* that their claim arose out of forum-directed activities, "personal jurisdiction is not established").

b. Plaintiffs' claims do not "arise out of" Ledger's forum-related activities

Because Plaintiffs cannot show that Ledger purposefully directed any activities at California, there are no "forum-related activities" by Ledger out of which Plaintiffs' claims arise.

Moreover, *Ledger's* practices or conduct with respect to the two security incidents at issue occurred in Paris, where Ledger is headquartered. *See Caces-Tiamson v. Equifax*, 2020 WL 1322889, at *3 (no specific jurisdiction where "all actions [the defendant] did or allegedly did not take with respect to its data security systems would presumably have occurred in . . . its [non-forum] principal place of business"). Neither Shopify Inc.'s nor Shopify (USA) Inc.'s conduct can establish personal jurisdiction as to Ledger. *See Walden v. Fiore*, 571 U.S. 277, 284 (2014) (quoting *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408, 417 (1984) ("[The] unilateral activity of another party or a third person is not an appropriate consideration when determining whether a defendant has sufficient contacts with a forum State to justify an assertion of jurisdiction").)[8] Without connecting their claims to any forum-related activity by Ledger, Plaintiffs cannot establish specific personal jurisdiction over it. *See, e.g.*, *Mocha Mill, Inc. v. Port of Mokha, Inc.*, No. 18-cv-02539-HSG, 2019 WL 1048252, at *5-6 (N.D. Cal. Mar. 5, 2019) (no personal jurisdiction where plaintiffs failed to show their claims arose out of defendant's contacts in California).

c. The exercise of jurisdiction over Ledger in California would be unreasonable

Because Plaintiffs cannot allege that Ledger purposefully directed activities intended to cause harm in California or that Plaintiffs' alleged injuries arose from any conduct in California, the personal jurisdiction inquiry should end there. *Schwarzenegger*, 374 F.3d at 802; *see also Hudson-munoz, LLC v. U.S. Waffle Co., Inc.*, No. 2:19-cv-01960-ODW (RAO), 2019 WL 3548919, at *4 (C.D. Cal. Aug. 5, 2019) ("As Plaintiff has not made a prima facie showing of the first two prongs of specific jurisdiction, the Court does not reach the issue of reasonableness."). If there were any doubt left, however, the exercise of personal jurisdiction over Ledger would be improper under the third and final unreasonableness prong. Because Plaintiffs fail to allege any California-related conduct by Ledger (and any harm suffered by Plaintiffs in California arising out of such conduct), all seven factors courts consider when making the reasonableness determination weigh heavily in Ledger's favor. *See CE Distribution, LLC v. New Sensor Corp.*, 380 F.3d 1107, 1112 (9th Cir. 2004) (courts consider "(1) the extent of the defendants' purposeful interjection into the forum state's affairs; (2) the burden on the defendant of defending in the forum; (3) the extent of conflict with the sovereignty of the defendants' state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum"). This is especially true given California's incidental (at best) interest in this matter: four of the five plaintiffs are outside of California (and two are international), no defendant is a resident of California, two out of the three defendants (Ledger and Shopify Inc.) are citizens of foreign countries, and no challenged conduct occurred here. *See Amoco Egypt Oil Co. v. Leonis Nav. Co., Inc.*, 1 F.3d 848, 852-53 (9th Cir. 1993). In addition, the arguments that support dismissing under the doctrine of *forum non conveniens* also support a finding that exercising jurisdiction over Ledger would be unreasonable.

---

[8] For the reasons set forth in Defendants' Shopify Inc.'s and Shopify (USA) Inc.'s motions to dismiss, Plaintiffs cannot establish jurisdiction as to either entity.

B. Plaintiffs Agreed to Multiple Forum Selection Clauses, Which Compel Dismissal of Their Claims

Through their purchase and continued use of Ledger's products and services, Plaintiffs agreed to Ledger's Privacy Policy, the Ledger Sales Terms and Conditions, and the Ledger Live Terms of Use, all of which contain forum selection clauses compelling Plaintiffs to litigate their claims in France. (Graniou Decl. ¶¶ 3-8; Ex. A at 13, Ex. B at 23, Ex. C at 41.) Each of these forum selection clauses is enforceable and requires dismissal of Plaintiffs' claims.

"The appropriate way to enforce a forum-selection clause pointing to a state or foreign forum is through the doctrine of *forum non conveniens*." *Atl. Marine Const. Co. v. U.S. Dist. Ct. for W. Dist. of Texas*, 571 U.S. 49, 60 (2013). "If the court finds that a dispute is covered by a forum selection clause, the forum selection clause should be enforced unless enforcement is shown by the resisting party to be unreasonable under the circumstances." *Livingston v. Pneu-Logic Corp.*, No. 20-cv-07155-JCS, 2021 WL 1375903, at *3 (N.D. Cal. Apr. 12, 2021). "On a motion to enforce a forum selection clause, the pleadings need not be accepted as true, and facts outside the pleadings may be considered." *Id.* at *4.

1. Plaintiffs’ claims are within the forum selection clauses

Privacy Policy. Ledger’s Privacy Policy—which serves as the predicate for all of Plaintiffs’ claims—contains a forum selection clause requiring that “any dispute” arising out of the Privacy Policy be “subject to the exclusive jurisdiction of the French courts.” (*See* FAC ¶ 53, n.5 (linking Ledger’s Privacy Policy); https://shop.ledger.com/pages/privacy-policy; Graniou Decl., ¶ 3, Ex. A at 13.) “[F]orum-selection clauses covering disputes ‘arising out of’ a particular agreement apply only to disputes relating to the interpretation and performance of the contract itself.” *Yei A. Sun v. Advanced China Healthcare, Inc.*, 901 F.3d 1081, 1086 (9th Cir. 2018). Here, Plaintiffs’ claims “arise out of” Ledger’s Privacy Policy because they challenge Ledger’s performance of the security measures outlined in the Privacy Policy and Ledger’s representations about the performance of those measures. (*See, e.g.,* FAC ¶¶ 53, 175, 180, 187, 203, 206, 207, 215, 218, 219, 233, 242, 251, 252, 262, 263, 274.)

Ledger Sales Terms and Ledger Live Terms. The Ledger Sales Terms contain a forum selection clause requiring that “any dispute relating to the application or interpretation of” the Sales Terms “be brought before the French court with material and territorial jurisdiction.” (Graniou Decl., ¶ 4, Ex. B at 23.) Likewise, the Ledger Live Terms contain a forum selection clause requiring that “any dispute, controversy, difference or claim arising out of or relating to [the Ledger Live Terms] . . . shall be referred to and finally resolved by the competent courts of Paris, France.” (*Id.*, ¶ 6, Ex. C at 41.)

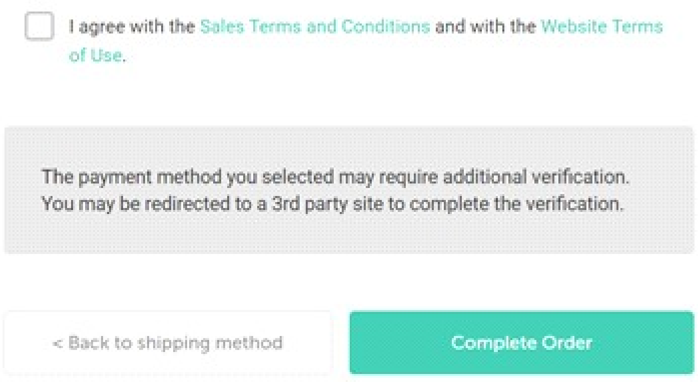
Where, like here, the “forum-selection clause[] cover[s] disputes ‘relating to’ a particular agreement” the clause “appl[ies] to any disputes that reference the agreement or have some logical or causal connection to the agreement.” *Yei A. Sun*, 901 F.3d at 1086. “The dispute need not grow out of the contract or require interpretation of the contract in order to relate to the contract.” *Id.* (forum selection clause containing the phrase “arising out of or related to” applies broadly to any dispute logically or causally connected to the agreement); *see also HSM Holdings, LLC v. Mantu I.M. Mobile Ltd.*, No. 19-cv-04391-JST, 2020 WL 7220462, at *3 (N.D. Cal. Jan. 30, 2020). Because the forum selection clauses in the Ledger Sales Terms and Ledger Live Terms cover any disputes “relating to” the terms, they cover claims that have any logical or causal connection to the terms. *See Yei A. Sun*, 901 F.3d at 1086.

The Ledger Sales Terms, among other things, "define the rights and obligations of the parties in connection with the sale of Products" on Ledger's website, govern Ledger's liability for "loss of profits, income, value or data, or indirect, special, consequential, exemplary, or punitive damages[,]" and discuss Ledger's processing and collection of personal data. (Graniou Decl., Ex. B at 16, 21, 22.) The Ledger Live Terms govern Ledger's liability for "damages for loss of profits, goodwill, use, data, cost of procurement of substitute goods or services, or other intangible losses, resulting from . . . the unauthorized access to or alteration of your transmissions or data" and "any other matter relating to [Ledger's] service." (*Id*., Ex. C at 39.) Accordingly, Plaintiffs' claims, which involve personal data they provided to Ledger during their purchase of Ledger products or services, are logically and causally connected to the Ledger Sales Terms and the Ledger Live Terms and are within the scope of the forum selection clauses contained therein.

2. The forum selection clauses are enforceable

The party challenging a forum selection clause "bears a heavy burden of proof and must clearly show that enforcement would be unreasonable." *Color Switch LLC v. Fortafy Games DMCC*, 377 F. Supp. 3d 1075, 1082 (E.D. Cal. 2019). The enforcement of Ledger's forum selection clauses is unreasonable only "if the party resisting enforcement makes a strong showing that: (1) the clause is invalid for such reasons as fraud or overreaching, (2) enforcement would contravene a strong public policy of the forum in which suit is brought, whether declared by statute or by judicial decision, or (3) proceeding in the selected forum will be so gravely difficult and inconvenient" that the complaining party "will for all practical purposes be deprived of his day in court." *Id.* Once a court finds that a forum selection clause is enforceable, "it must balance public interest factors to determine whether dismissal of the action in favor of the other forum would promote justice." *Color Switch LLC*, 377 F. Supp. 3d at 1083. Plaintiffs cannot meet this heavy burden here.

First, Plaintiffs have no basis to argue that they did not assent to the forum selection clauses or that the clauses are the product of fraud or overreaching. Before purchasing their hardware wallets, Ledger provided Plaintiffs the Sales Terms via hyperlink and gave them the opportunity to review the terms in full. (Graniou Decl. ¶ 5.) To complete their purchases, Plaintiffs were required to affirmatively click a check box indicating their agreement to the Sales Terms, as demonstrated in this screen shot of the current Ledger website checkout process:



☐ I agree with the Sales Terms and Conditions and with the Website Terms of Use.

The payment method you selected may require additional verification. You may be redirected to a 3rd party site to complete the verification.

(*Id.*) Likewise, before Plaintiffs could use Ledger Live, Ledger provided Plaintiffs the Ledger Live Terms and Privacy Policy via hyperlink and gave them the opportunity to review both in full. (*Id.* ¶ 7.) As with the Sales Terms, users of the Ledger Live App are required to affirmatively click separate check boxes indicating their agreement to the Ledger Live Terms and Privacy Policy. (*Id.*) Finally, to continue using the App, Plaintiffs were required to "re-accept" the Ledger Live Terms each time Ledger updated the terms. (*Id.* ¶ 8.) Finally, independently of the Ledger Live App, Plaintiffs assented to the Privacy Policy, which is hyperlinked at the bottom of every page on Ledger's website (*id.* ¶ 3) and on which Plaintiffs rely for their claims, by using Ledger's services. (*See* FAC ¶ 53 n.5 (linking Ledger's Privacy Policy); https://shop.ledger.com/pages/privacy-policy ("If you do not agree with or you are not comfortable with any aspect of this Privacy Policy, you should immediately discontinue access or use of our Services")[9]; *see also* Graniou Decl., Ex. A at 5.)

---

[9] "[C]ourts must consider the complaint in its entirety," including "documents incorporated into the complaint by reference." *See Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007). The incorporation-by-reference doctrine "prevents plaintiffs from selecting only portions of documents that support their claims, while omitting portions of those very documents that weaken — or doom — their claims." *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002 (9th Cir. 2018), *cert. denied*, *Hagan v. Khoja*, 139 S. Ct. 2615 (2019). Plaintiffs reference and cite Ledger's Privacy Policy in the FAC (FAC ¶ 53); it is thus proper for the Court to consider Ledger's Privacy Policy in its entirety, including the portions Plaintiffs chose not to include. *See, e.g., In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1058 n.10 (9th Cir. 2014) (the

Courts uphold forum selection clauses where, like here, the clause is in a website or app's click-through user agreement or a browsewrap agreement. *Thomas v. Facebook*, No. 1:18-cv-00856-LJO-BAM, 2018 WL 3915585, at *4 (E.D. Cal. Aug. 15, 2018) (presumption of enforceability "has been consistently and routinely applied to forum selection clauses contained in click through user agreements on websites"); *see also Meier v. Midwest Recreational Clearinghouse*, LLC, No. 2:10-cv-01026-MCE-GGH, 2010 WL 2738921, at *3 (E.D. Cal. July 12, 2010) (enforcing forum selection clause contained in click-wrapped terms of service on auction website); *Cairo, Inc. v. Crossmedia Services, Inc.*, No. C 04-04825 JW, 2005 WL 756610 (N.D. Cal. Apr. 1, 2005) (enforcing forum selection clause in a browsewrap agreement because Plaintiff admitted to being aware of the agreement/terms and visited the website while aware of the agreement/terms). Here, the Sales Terms and Ledger Live Terms are click-through agreements and Ledger's Privacy Policy is both a browse-wrap and a click-through agreement. Accordingly, the forum selection clauses in all three should be enforced. That each of Ledger's forum selection clauses is contained in "a form contract does not render its terms fraudulent or the product of overreaching." *Sawyer v. Bill Me Later, Inc.*, No. CV 10-04461 SJO (JCGx), 2010 WL 5289537, at *5 (C.D. Cal. Oct. 4, 2010) ("This Court cannot vitiate a valid [forum selection clause] because of an imbalance of bargaining power for a nonnegotiable contract"); *LaCross v. Knight Transportation, Inc.*, 95 F. Supp. 3d 1199, 1203 (C.D. Cal. 2015) (same).

Second, Plaintiffs cannot establish that enforcement of the forum selection clauses will contravene a strong public policy in California because Ledger's Privacy Policy, the Sales Terms, and Ledger Live Terms do not preclude Plaintiffs from pursuing their claims under California law. (Graniou Decl. Ex. A at 13, Ex. B at 23, Ex. C at 41.) For that reason, Plaintiffs cannot argue that enforcing the forum selection clause will violate the anti-waiver provision of the CLRA. Courts enforce forum selection clauses in cases involving CLRA claims, where, as here, the plaintiffs' CLRA rights are not impacted because they are free to pursue claims under California law in the designated forum. *See Scott v. Jayco, Inc.*, No. 1:18-cv-00861-LJO-JLT,

---

full text of documents referenced or cited in a complaint may be considered even though the complaint quotes only portions of those documents).

2018 WL 5816153, at *4 (E.D. Cal. Nov. 5, 2018); *Brooks v. Sotheby's*, No. 13-cv-02183 RS, 2013 WL 3339356, at *3 (N.D. Cal. July 1, 2013) (no violation of CLRA anti-waiver provision where "the governing law provisions do not preclude application of California law in the designated forum, and [plaintiff] is free to argue California law should govern this dispute under English conflict of law rules"); *Mazzola v. Roomster Corp.*, No. CV 10-5954 AHM (JCGx) 2010 WL 4916610, at *3 (C.D. Cal. Nov. 30, 2010) (no violation of CLRA anti-waiver provision where plaintiff is free to argue for application of California law once in the proper venue).

Third, Plaintiffs are unable to show that they would be deprived of their day in court if they were to litigate in the designated forum—France. "To meet the heavy burden required to overcome the presumption that a forum selection clause is valid, [a] plaintiff must show that it is an impossibility for her to try her case, not simply a less convenient or effective means of doing so." *Lightfoot v. MoneyonMobile, Inc.*, No. 18-CV-07123-YGR, 2019 WL 2476624, at *6 (N.D. Cal. June 13, 2019). Here, it is neither less convenient nor less effective to litigate in France, let alone impossible. All but one of Plaintiffs are either closer to France than they are to California (Plaintiffs Deeney and Vilinger) or roughly equidistant from France and California (Plaintiffs Baton and Comilla). Plaintiffs are free to seek the exact same relief they are pursuing here, as the forum selection clause does not bar Plaintiffs from bringing claims under California law. Moreover, even if it did, French law would afford Plaintiffs adequate relief. *See MGA Ent. Inc. v. Deutsche Bank AG*, No. CV 11-4932 GW (RZX), 2012 WL 12892902, at *3 (C.D. Cal. Feb. 27, 2012) (courts "generally have found France's judicial system to be adequate" and a foreign forum "need not offer the same, or as favorable, remedies to still be adequate"); Law No. 2014-344 of 17 March 2014 (permitting consumer and competition related class-actions; Law No. 2016-1547 of 18 November 2016 (permitting personal data protection related class-actions). Accordingly, Plaintiffs will not be "deprived of their day in court" if the forum selection clauses are enforced.

3. The public interest factors weigh in favor of enforcing the forum selection clause and dismissing the case

The public interest factors the Court must consider include "the administrative difficulties flowing from court congestion; the local interest in having localized controversies decided at home; and the interest in having the trial of a diversity case in a forum that is at home with the law." *Color Switch LLC*, 377 F. Supp. 3d at 1091. That said, "the consideration of public interest factors alone will rarely defeat a forum selection clause." *Id.*; *see also Atl. Marine Const. Co.*, 571 U.S. at 51 ("public-interest factors will rarely defeat a transfer motion" and "forum-selection clauses should control except in unusual cases").

Here, the public interest factors favor enforcing the forum selection clause. Although California may have an interest in providing its residents with a forum for redressing injuries, when "defendants are not California corporations, California has little interest in keeping the litigation in this state to deter future wrongful conduct." *Moretti v. Hertz Corp.*, No. C 13-02972 JSW, 2014 WL 1410432, at *5 (N.D. Cal. Apr. 11, 2014). "The lack of evidence that any of the alleged activities actually took place in California" further weighs against California's interest in keeping this case in state. *Id.* Additionally, Plaintiffs allege a number of claims under laws of other states, suggesting that California is not "at home with the law."

4. Even without considering the forum selection clauses, Plaintiffs' claims should be dismissed on *forum non conveniens* grounds

Under the doctrine of *forum non conveniens*, courts may decline to exercise jurisdiction in favor of a more convenient forum outside the United States where, as here: (1) there exists an adequate alternative forum, and (2) that the balance of private and public interest factors favors dismissal. *Creative Tech. Ltd. v. Aztech Sys. PTE, Ltd.*, 61 F.3d 696, 703 (9th Cir. 1995). An alternative forum is adequate if "(1) the defendant is amenable to process there; and (2) the other jurisdiction offers a satisfactory remedy." *Carijano v. Occidental Petroleum Corp*., 643 F.3d 1216, 1225 (9th Cir. 2011) (citing *Piper Aircraf Co. v. Reyno*, 454 U.S. 235, 254 n.22 (1981)). That is exactly the case here. Ledger is amenable to service in France as it is incorporated and headquartered there, and as established above, the French court system will provide Plaintiffs an avenue for redress. *See MGA Ent. Inc.*, 2012 WL 12892902, at *3 (acknowledging that courts "generally found France's judicial system to be adequate"); *see also Lueck v. Sundstrand Corp.*, 236 F.3d 1137, 1144 (9th Cir. 2001) ("a foreign forum will be deemed adequate unless it offers no practical remedy for the plaintiff's complained of wrong").

The private and public interest factors also favor dismissal. As detailed above, Plaintiffs' claims have no substantive connection to California. Only one of the five plaintiffs is a California resident, the conduct at issue as it relates to Ledger occurred in France, the security measures at issue in Plaintiffs' claims against Ledger and representations about those measures were all adopted in France, all evidence about the measures is located in France, and the majority of the witnesses who can testify about these issues are located in France. The value of one named plaintiff's testimony—the only relevant witness connected to California—is greatly outweighed by the need for evidence from witnesses and documents located abroad. *See Ruelas Aldaba v. Michelin North America, Inc.*, No. C 04–5369 MHP, 2005 WL 3560587, at *5-9 (N.D. Cal. Dec. 29, 2005) (dismissing for *forum non conveniens* even though three of the fifteen plaintiffs resided in California because witnesses and documentary evidence were in Mexico, the "action's center of gravity [was] in Mexico[,]" and Mexico had a strong interest in litigating the action). These facts suggest that the "practical problems" of this case will make trial in Plaintiffs' chosen forum anything but "easy, expeditious, [or] inexpensive." *Lueck*, 236 F.3d at 1145-46 (quoting *Gulf Oil Corp. v. Gilbert*, 330 U.S. 501, 508 (1947)).

C. The FAC Fails to State a Claim

A court must dismiss a complaint for failure to state a claim under Rule 12(b)(6) when, as here, Plaintiffs either fail to state a cognizable legal theory or have not alleged sufficient facts establishing a claim to relief that is "plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "[C]onclusory allegations without more are insufficient to defeat a motion to dismiss . . . ." *McGlinchy v. Shell Chem. Co.*, 845 F.2d 802, 810 (9th Cir. 1988). Thus, the Court must not assume the truth of legal conclusions merely because they are pleaded in the form of factual allegations, nor should it accept as true allegations contradicted by judicially noticeable facts. *Iqbal*, 556 U.S. at 677-79; *Twombly*, 550 U.S. at 555.[10]

---

[10] Plaintiffs all purport to bring claims under California law, despite the fact that four out of five of them do not reside in California, and of those four, two live outside the United States. (FAC ¶¶ 16-20.) Ledger reserves the right to challenge whether California law governs the non-resident Plaintiffs' claims.

Rule 9(b)'s heightened pleading standard also applies to Plaintiffs' claims. The crux of Plaintiffs' claims is that Ledger misrepresented the security of its hardware wallets and that Ledger (and Shopify) failed to prevent the security incidents. (FAC ¶¶ 6, 12, 14.) Because each of Plaintiffs' claims is grounded in fraud, "the pleading . . . as a whole must satisfy the particularity requirement of Rule 9(b)." *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124-25 (9th Cir. 2009) (quotations and citation omitted). All "averments of fraud" must be specifically pled "irrespective of whether the substantive law at issue is state or federal," and even where "fraud is not an essential element of a claim." *Id.*

1. Plaintiffs' UCL and CLRA claims, which sound in fraud, fail

a. Plaintiffs have not identified any statements likely to deceive a reasonable consumer

To state a claim under the UCL and CLRA, Plaintiffs must specifically identify a representation likely to deceive the public. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 967-68 (S.D. Cal. 20112) ("*Sony*") (dismissing UCL claim where plaintiffs failed to show how representations, taken as a whole, would be likely to deceive the reasonable consumer). "Likely to deceive implies more than a mere possibility that the advertisement might conceivably be misunderstood by some few consumers viewing it in an unreasonable manner." *Lavie v. Procter & Gamble Co.*, 105 Cal. App. 4th 496, 508 (2003). Rather, "likely to deceive" indicates "it is probable that a significant portion of the general consuming public or of targeted consumers, acting reasonably in the circumstances, could be misled" by the statement. *Id.* Rule 9(b) requires Plaintiffs to "set forth what is false or misleading about a statement, and why it is false." *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003). Plaintiffs do not identify any statements Ledger made about the security of its e-commerce database, the Shopify incident, or Ledger cyber attack that are likely to deceive a reasonable consumer.

***Representations Regarding Personal Data Are Not Misleading*.** Plaintiffs selectively quote from Ledger's Privacy Policy to support their allegation that Ledger misrepresented that consumers' "personal data…will remain anonymous, secure, and private." (FAC ¶ 6.) Despite quoting it in the FAC, they ignore that Ledger discloses the existence of a security risk in the Policy: "While we endeavor to provide best-in-class protection for your personal data . . . , please keep in mind that the transmission of information on the Internet is not fully secure." (*Id.*)

Sony, which considered similar language in a privacy policy, compels dismissal of Plaintiffs' claims. There, the plaintiffs alleged Sony misrepresented the quality of its network security after the network was hacked. *Sony,* 903 F. Supp. 2d at 968. Sony's privacy policy, much like Ledger's, stated that "there is no such thing as perfect security ... we cannot ensure or warrant the security of any information transmitted to us through [the Sony network] ..." *Id.* The court dismissed the UCL and CLRA claims finding that no reasonable consumer could have been deceived given Sony's "clear admonitory language that [its] security was not 'perfect.'" *Id.* The same reasoning requires dismissal here.

Representations Regarding Hardware Wallets Are Not Misleading. Plaintiffs cannot rely on Ledger's representations about the security of the hardware wallets to support their claims because the statements clearly describe the hardware wallets, not the e-commerce database that was hacked. Plaintiffs point to statements that Ledger "has the 'highest security standards,' that it 'continuously look[s] for vulnerabilities on Ledger products as well as our providers' products in an effort to analyze and improve the security," and the hardware wallets provide "the highest level of security for crypto assets." (FAC ¶¶ 6, 68-71.) Each of these statements pertain to the technology used for the hardware wallets. Plaintiffs do not allege that their hardware wallets were hacked or that cyber-criminals accessed the passwords protecting their crypto assets. As such, statements about the security of the hardware wallets are irrelevant and cannot form the basis of Plaintiffs' claims.

Representations Regarding Cyber Attacks Are Not Misleading. Finally, Ledger's statements about the security incidents also cannot support Plaintiffs' claims. Plaintiffs allege Ledger's May 24, 2020 tweet regarding its investigation into rumors of a data breach and July 29, 2020 statement about the Ledger cyber attack were false and misleading. (FAC ¶¶ 86, 88, 218). Not so. Reasonable consumers understand the tweet to mean what it said: Ledger was investigating rumors of a cyber attack and did not yet know if there had been a breach. Ledger's

July 29 statement regarding the Ledger cyber attack is also clear; it accurately informed the public about the information disclosed in the cyber attack. Plaintiffs do not allege any facts showing that either the tweet or the statement contained any false or misleading information, including with respect to the type or scope of contact information impacted.

Plaintiffs implausibly contend Ledger's July 29 announcement was incomplete because "Ledger did not disclose that this breach had anything to do with the Shopify breaches." (FAC ¶ 91.) Their other allegations show, however, that the cyber attack Ledger disclosed on July 29 was ***unrelated*** to the Shopify incident. (*Compare* FAC ¶ 88 (on June 25 an unauthorized third party accessed Ledger's e-commerce and marketing database) *with id.* ¶¶ 78-79 ("between April and June" two rogue Shopify "employees" exported Ledger's customer transactional records).) Indeed, the "E-commerce and Marketing data breach – FAQ" from ledger.com ("Ledger FAQs")[11] they cite indisputably show that Ledger did not learn that the rogue Shopify "employees" also stole Ledger customer records until December 21, 2020. (FAC ¶ 82, n. 8 (citing Ledger FAQs).)[12] Plaintiffs' allegations reveal that Ledger could not have disclosed the Shopify incident in July 2020. Shopify did not publicly announce the incident until two months later in September 2020 (*id.* ¶ 79), and Ledger did not learn that the incident affected its customers until five months later in December 2020 (*id.* ¶ 82, n. 8). As such, Plaintiffs cannot identify any false or misleading statement about either security incident.

b. Plaintiffs have not alleged exposure or reliance

Actual reliance is a statutory element of Plaintiffs' UCL and CLRA claims, and Plaintiffs' failure to plead exposure, reliance, and causation is fatal to their claims. *See Sateriale v. R.J.*

---

[11] The Ledger FAQs are available at https://support.ledger.com/hc/en-us/articles/360015559320-E-commerce-and-Marketing-data-breach-FAQ?support=true (last visited July 26, 2021).

[12] Because Plaintiffs reference and cite the Ledger FAQs regarding the Shopify incident and Ledger cyber attack (FAC ¶ 82, n. 8.), the Court may consider the FAQs in their entirety. *See, e.g., In re NVIDIA Corp. Sec. Litig.,* 768 F.3d at 1058 n.10 (the full text of documents cited in a complaint may be considered even though the complaint quotes only portions of those documents). Moreover, courts routinely recognize corporate websites under the incorporation by reference doctrine where the plaintiff puts a component of the website, or something determinable therein, at issue. *Haskins v. Symantec Corp.*, No. 13-cv-01834-JST, 2013 WL 6234610, at *1 n.1 (N.D. Cal. Dec. 2, 2013) (considering documents from corporate defendant's website).

Reynolds Tobacco Co., 697 F.3d 777, 793 (9th Cir. 2012) (for claims sounding in fraud, reliance must be pleaded with the particularity required by Rule 9(b)). Plaintiffs must allege that they saw an actionable statement and took action based on what they saw. *See In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *28 (N.D. Cal. Aug. 30, 2017) (dismissing fraud-based UCL claim because plaintiffs did not allege that they "actually read" or relied on the alleged misrepresentation); *Baltazar v. Apple, Inc.*, No. CV-10-3231-JF, 2011 WL 588209, at *4 (N.D. Cal. Feb. 10, 2011) (dismissing CLRA claim because plaintiffs had not "alleged that they relied justifiably on [the alleged] misrepresentations") (citations omitted).

Plaintiffs do not identify any allegedly misleading statement they saw or relied on when they purchased a Ledger hardware wallet or after the security incidents. Plaintiff Seirafi generally alleges he "saw advertisements online" and relied on advertised "data security services" when he bought his Ledger Nano X. (FAC ¶ 16). The other Plaintiffs allege they relied on purported "misrepresentations about the security of [Ledger's] products" when they purchased their hardware wallets. (FAC ¶¶ 17-20.) No Plaintiff, however, offers a single detail regarding any specific representation(s) they saw, read, and relied on when purchasing a hardware wallet. They further do not allege that they read or relied on Ledger's Privacy Policy, any statements on Ledger.com, or any alleged Ledger statements about the "lack of the data breach" and the "extent of the breach" that they assert are misleading. (FAC ¶ 218.) Because Plaintiffs do not allege exposure or reliance, the Court should dismiss their UCL and CLRA claims. *See Pirozzi v. Apple Inc.*, 913 F. Supp. 2d 840, 850 (N.D. Cal. 2012) (dismissing UCL and CLRA claims where plaintiff failed to provide the particulars of her own experience reviewing or relying on any of the alleged misrepresentations); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *37 (N.D. Cal. May 27, 2016) (dismissing UCL claim where no plaintiff alleged they saw, read, or knew about defendant's alleged misrepresentations).

c. Plaintiff Seirafi lacks UCL and CLRA statutory standing because he does not allege injury

Under the UCL, standing is limited to those who "lost money or property" as a result of unfair competition. Cal. Bus. & Prof. Code § 17204; *see also Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 322 (2011). Likewise, the CLRA affords relief only to California consumers "who suffer[] . . . damage as a result of the use . . . by any person of a method, act, or practice declared to be unlawful by Section 1770[.]" Cal. Civ. Code § 1780(a); *Meyer v. Sprint Spectrum L.P.*, 45 Cal. 4th 634, 641 (2009). Plaintiff Seirafi does not meet these requirements.[13]

First, Seirafi does not allege any loss of money or property or damage, including as to his cryptocurrency assets, as a result of either security incident. He has not been the victim of identity theft or fraud, and his allegations regarding SIM-swap attacks, ransom threats, and phishing emails fail to establish standing. (*See*, *infra*, Section IV.D(2)); *see also Sony*, 903 F. Supp. 2d 942, 966 ("heightened risk of identity theft, time and money spent on mitigation of that risk, and property value in one's information, do not suffice as injury under the UCL . . . and/or the CLRA"); *Flores-Mendez v. Zoosk, Inc.*, No. C 20-04929 WHA, 2021 WL 308543, at *4 (N.D. Cal. Jan. 30, 2021) (no injury under UCL when plaintiff alleged loss of privacy, heightened risk of future identity theft, loss of time, and anxiety). Nor does the disclosure of personal information constitute a loss of money or property. *See Sony*, 903 F. Supp. 2d at 965-66 (no UCL standing based on alleged compromise of personal information); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1126 (N.D. Cal. 2008), *aff'd*, 380 F. App'x 689 (9th Cir. 2010) (unauthorized release of personal information does not constitute a loss of property sufficient to state UCL claim).

Second, Seirafi cannot predicate his UCL or CLRA claim on the money he paid to purchase his Ledger Nano X. There is no causal relationship between the alleged wrongdoing underlying his claims (the alleged failure to secure his contact information) and his alleged damages (he purchased or paid more for a hardware wallet than he otherwise would have). (FAC ¶¶ 207-210.) Seirafi alleges no defect in the Ledger Nano X he purchased, which he presumably has used without incident. He does not allege in any fashion, much less in a concrete fashion, that he did not want the Ledger Nano X, that it was itself hacked or otherwise unsatisfactory, that it was worth less than he paid, or that he could have purchased it cheaper elsewhere. *See, e.g.*, *Peterson v. Cellco Partnership*, 164 Cal. App. 4th 1583, 1591 (2008). Because Seirafi does not allege he lost money or property or was damaged due to either security incident, the Court should dismiss his UCL and CLRA claims.

---

[13] If this case proceeds past the pleading stage, it is unlikely that the other Plaintiffs will be able to prove injury, causation, or damage, either.

2. Plaintiffs fail to state a claim for deceit by concealment

To assert a claim for deceit by concealment under Cal. Civ. Code §§ 1709 and 1710, Plaintiffs must show (i) Ledger was under a duty to disclose a fact to them, (ii) Ledger intentionally concealed or suppressed that fact with the intent to defraud them, and (iii) that they were unaware of the fact and would not have acted as they did had they known of the concealed fact. *Tae Youn Shim v. Lawle*r, No. 17-CV-04920-EMC, 2019 WL 2996443, at *17 (N.D. Cal. July 9, 2019), *appeal dismissed*, No. 19-16539, 2020 WL 529711 (9th Cir. Jan. 24, 2020). A duty to disclose arises in four circumstances: "(1) when the defendant is in a fiduciary relationship with the plaintiff; (2) when the defendant had exclusive knowledge of material facts not known to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; and (4) when the defendant makes partial representations but also suppresses some material facts." *Grisham v. Philip Morris, Inc.*, 670 F. Supp. 2d 1014, 1043 (C.D. Cal. 2009) (internal quotation marks omitted). Because deceit by concealment "sounds in fraud," Plaintiffs must "state with particularity the circumstances constituting fraud" under Rule 9(b). *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 800 (N.D. Cal. 2019). Plaintiffs assert that Ledger had a duty to disclose that its security system was "not adequate to safeguard consumers' PII" and "concealed the breach" (FAC ¶¶ 241, 243), but do not plead facts to support a legal basis for this duty.

"Commercial, arms-length relationships" like the ones between Plaintiffs and Ledger are not fiduciary. *Grisham*, 670 F. Supp. 2d at 1043. Nor do Plaintiffs plead any facts showing that Ledger exclusively knew that its security systems were not adequate. In fact, Plaintiffs acknowledge that Ledger's Privacy Policy discloses "the transmission of information on the Internet is not fully secure." *See Terpin v. AT&T Mobility, LLC*, No. 2:18-cv-06975-ODW (KSx), 2020 WL 5369410, at *3 (C.D. Cal. Sept. 8, 2020) (no exclusive knowledge of security system when privacy policy disclosed that the system was subject to inadequacies).

Plaintiffs also do not allege any facts showing that Ledger actively concealed anything from them. Active concealment requires the party to take "affirmative acts…in hiding, concealing, or covering up the matters complained of." *Czuchaj v. Conair Corp*., No. 13-CV-1901-BEN (RBB), 2014 WL 1664235, at *6 (S.D. Cal. Apr. 18, 2014) (internal quotation marks omitted). Plaintiffs generally conclude Ledger "concealed" the Shopify incident, but plead no "affirmative acts" Ledger took to conceal information about the security of Ledger's e-commerce database or either security incident. They do not assert that Ledger knew about the misconfigured API key before July 14, 2020, much less hid it. (FAC ¶¶ 88.) In fact, Plaintiffs admit that Ledger promptly notified all affected individuals about the Ledger cyber attack and continues to update customers about the incidents. (*See id.* (alleging Ledger informed the public of the Ledger cyber attack within two weeks); *id* ¶ 82 n.8 (citing to Ledger FAQs).)

Plaintiffs' allegations confirm that Ledger's July 29, 2020 announcement regarding the Ledger cyber attack was not a partial admission that suppressed a material fact. As discussed above, the Ledger FAQs they cite ***disprove*** their assertion that Ledger should have disclosed on July 29 that (1) the Ledger cyber attack was related to the Shopify incident and (2) the "status and dissemination of the stolen data." (FAC ¶¶ 82, n. 8, 91-92; *see*, *supra*, Section IV.C(1)(a).) Indeed, Ledger did not learn of the Shopify incident until December 21, 2020. (*See* FAC ¶ 82, n. 8.) Thus, it was impossible for Ledger to disclose in July 2020 that its customers' contact information was involved in the Shopify incident. (*Id.*) Plaintiffs also do not allege—nor could they—that Ledger knew how the unknown criminals planned to use or disseminate the information they stole from Ledger's e-commerce database. Because Plaintiffs do not allege Ledger had a duty to disclose any additional information about its security systems or plead facts showing that Ledger concealed either security incident, the Court should dismiss their claim.

3. Plaintiffs fail to state a claim for negligence and negligence per se

To state a negligence claim, Plaintiffs must allege: (1) the existence of a duty to exercise due care; (2) breach of that duty; (3) causation; and (4) damages. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d at 959-60 (citing *Paz v. Cal.*, 22 Cal. 4th 550, 558 (2000)). Plaintiffs' negligence claim fails because they do not plausibly allege Ledger breached any duty that proximately caused their alleged injuries. Plaintiffs' negligence per se claim also fails because it is not cause of action and it "does not provide a private right of action for violation of a statute." *Quiroz v. Seventh Ave. Ctr.*, 140 Cal. App. 4th 1256, 1285 (2006). Even if California law permits Plaintiffs to bring a standalone negligence per se claim, the claim would fail on the same grounds as their negligence claims. *See Dent v. Nat'l Football League*, 968 F.3d 1126, 1132 (9th Cir. 2020) (affirming dismissal of per se theory of negligence).

a. Plaintiffs do not allege Ledger breached any duty

Plaintiffs cannot state a claim for negligence based on the unsupported conclusion that Ledger failed to "exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the personal information of the Class members;" "detect the breaches while they were ongoing;" "maintain security systems consistent with industry standards;" and "disclose that the…personal information in Ledger's….possession had been or was reasonably believed to have been stolen or compromised." (FAC ¶ 175). "It is well established that the occurrence of an unfortunate event is not sufficient to authorize an inference of negligence." *Willingham v. Glob. Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *19 (N.D. Ga. Feb. 5, 2013) (internal citation and quotation omitted) (dismissing negligence claim based on alleged harm resulting from data breach). Plaintiffs do not plausibly allege a breach of any duty.

Plaintiffs point to an "unfortunate event" and asks the Court to infer negligence, without pleading a single fact that shows that Ledger did not institute adequate security measures, maintain industry standard security systems, or disclose the security incidents.[14] Plaintiffs fail to assert what security measures Ledger employed, how Ledger's security practices departed from reasonable or adequate standards of care, or how different industry-standard practices could have detected the cyber attack or prevented criminals from stealing Plaintiffs' information. "The implied premise that because data was hacked [the company's] protections must have been inadequate is a 'naked assertion[ ] devoid of further factual enhancement' that cannot survive a motion to dismiss." *See Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717 (8th Cir. 2017) (dismissing breach of contract claim for failure to adequately allege breach); *Anderson v. Kimpton Hotel & Rest. Grp., LLC*, No. 19-cv-01860-MMC, 2019 WL 3753308, at *5 (N.D. Cal. Aug. 8, 2019) (granting motion to dismiss where "plaintiffs fail to allege any facts in support of their conclusory assertion that [defendant] . . . 'fail[ed] to implement and maintain reasonable security procedures and practices'"); *Razuki v. Caliber Home Loans, Inc.*, No. 17cv1718-LAB (WVG), 2018 WL 6018361, at *1–2 (S.D. Cal. Nov. 15, 2018) (plaintiff's "claims 'Defendant knew of higher-quality security protocols available to them' but failed to implement these measures . . . fail[] because it is precisely the type of 'threadbare' claim *Iqbal* warns of"). No matter how many times Plaintiffs repeat their conclusory allegations regarding a lack of adequate security measures, they cannot plausibly state a claim for negligence without alleging what security measures Ledger employed and how they were inadequate.

---

[14] Plaintiffs' conclusory allegation that Section 5 of the FTC Act establishes the applicable standard of care and that Ledger breached it is also insufficient. Under California law, a statute only creates a standard of care for a negligence claim only when its violation causes "death or injury to person or property" (among other requirements). Cal. Evid. Code § 669(a).

Second, Plaintiffs' assertion that Ledger breached its duty to them by providing untimely notice of the security incidents fares no better. (FAC ¶ 175.) Plaintiffs allege that they received notice of the Ledger cyber attack about two weeks after it happened. (*Id.* ¶ 88.) They do not explain why this notice was inadequate, what time period would have been satisfactory, or what they would have done differently that they did not do or could not do when they received notice. The FAQs they cite also show that Ledger promptly notified the public of the Shopify incident once it became aware of it. (*Id.* ¶ 82 n. 8 (citing Ledger FAQs).) As such, these conclusory allegations too are insufficient. *See Bem v. Stryker Corp.*, No. C 15-2485 MMC, 2015 WL 4573204, at *1 (N.D. Cal. July 29, 2015) (dismissing negligence claims where plaintiff failed to plead facts demonstrating how the defendant was negligent).

b. Plaintiffs' purported injuries are not fairly traceable to any duty they allege Ledger breached

Proximate cause "limits the defendant's liability to those foreseeable consequences that the defendant's negligence was a substantial factor in producing." *Mendoza v. City of Los Angeles*, 66 Cal. App. 4th 1333, 1342 (1998). When, as here, a third party's independent illegal act causes a plaintiff's alleged injury, there can be no proximate cause. *O'Keefe v. Inca Floats,* *Inc.*, No. C-97-1225 VRW, 1997 WL 703784, at *4 (N.D. Cal. 1997). Plaintiffs generally allege that Ledger's "negligence was, at least, a substantial factor in causing…Class members' other injuries as a result of the data breaches" (FAC ¶ 176), but their other allegations clearly show that criminal actors, not Ledger, are to blame (*id.* ¶¶ 99, 103, 116, 128). Each of their alleged injuries only occurred because criminals independently chose to steal Ledger customer contact information and then illegally use it to send phishing communications and threaten Ledger's customers. In addition to failing to show Ledger negligently maintained the security of its customers' contact information, Plaintiffs' threadbare allegations do not establish that any negligent act by Ledger caused any of Plaintiff's alleged injuries.

4. Plaintiff Baton's Georgia Fair Business Practices Act and Uniform Deceptive Trade Practices Act claims fail

The gravamen of Plaintiff Baton's GFBA and GUDTPA claims is that Ledger failed to safeguard his personal information and misrepresented the security of its e-commerce database. (FAC ¶¶ 251, 262.) The Court should dismiss these claims because (1) these Georgia statutes do not impose a duty on Ledger to protect Baton's contact information; (2) Baton fails to plead reliance for his GFBPA claim; and (3) Baton has no available remedy under the GUDTPA.

a. The GFBPA and GUDTPA do not require Ledger to safeguard Baton's personal information

The Court should dismiss Baton's GFBPA and GUDTPA claims based on Ledger's alleged failure to implement and maintain security and privacy measures because "[t]here is no statutory basis for a duty to safeguard personal information in Georgia." *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1328–29 (N.D. Ga. 2019). In *In re Equifax*, the plaintiffs claimed Equifax did not implement adequate cyber-security practices, leading to the disclosure of the personally identifiable information of approximately 147.0 million consumers. 362 F. Supp. 3d at 1310. The court dismissed the GFBPA and GUDTPA claims on the ground the GFBPA "along with the rest of Georgia statutory law [does] not require the safeguarding of personal information." *Id.* at 1329 (citing *McConnell v. Dep't of Lab.*, 345 Ga. App. 669, 678 (2018), *aff'd*, 305 Ga. 812, 828 S.E.2d 352 (2019).) Baton's claims should likewise be dismissed.

b. Baton's GFBPA misrepresentation claim fails because he does not plead reliance

To state a misrepresentation claim under the GFBPA, a plaintiff "must demonstrate that he was injured as the result of [his] reliance upon the alleged misrepresentation." *Tiismann v. Linda Martin Homes Corp.*, 281 Ga. 137, 138 (2006) (quoting *Zeeman v. Black*, 156 Ga. App. 82, 87 (1980).) Baton does not assert, however, that he relied on any statements about the security of Ledger's e-commerce database. He generally alleges that he relied on "misrepresentations about the security of [Ledger's] products" (FAC ¶ 17), but does not identify a single statement he allegedly saw or relied on. (*See, supra*, Sections IV.C(1)(b).) Moreover, any statement Baton may have relied on regarding the security of the hardware wallets has no bearing on the security of Ledger's e-commerce database, which was the subject of the security incidents. (*See, supra*, Sections IV.C(1)(a).) Because Baton does not allege reliance, his GFBPA claim must be dismissed. *See In re Arby's Rest. Grp. Inc. Litig.,* No. 1:17-cv-0514-AT, 2018 WL 2128441, at *21 (N.D. Ga. Mar. 5, 2018) (dismissing GFBPA claim where plaintiffs did not allege actual reliance on defendant's alleged representations).

c. Baton is not entitled to injunctive relief under the GUDTPA

"[T]he sole remedy available under the [Georgia] UDTPA is injunctive relief." *Moore-Davis Motors, Inc. v. Joyner*, 252 Ga. App. 617, 619 (2001). Courts dismiss GUDTPA claims when plaintiffs fail to allege a future harm caused by the alleged unfair practice. *See, e.g.*, *Collins v. Athens Orthopedic Clinic*, 356 Ga. App. 776, 780 (2020) (affirming dismissal of GUDTPA claim based on data breach where plaintiffs did not allege future harm); *Terrill v. Electrolux Home Prod., Inc.*, 753 F. Supp. 2d 1272, 1291-92 (S.D. Ga. 2010) (dismissing GUDTPA claim "based entirely on past wrongs" when plaintiffs "do not allege that they will be damaged in the future…much less allege *how* they will be damaged"). Because Baton's alleged injuries are all based on alleged past harms and he does not plausibly allege imminent risk of any future injury, his GUDTPA claim must be dismissed.

Collins is on all fours. There, the plaintiffs alleged the defendant violated the GUDTPA by "failing to provide fair, reasonable, or adequate computer systems and data security practices," which they asserted resulted in a data breach that disclosed their personal information. *Collins*, 356 Ga. App. at 780. The Georgia Court of Appeals affirmed dismissal of the GUDTPA claim finding "an injunction would serve no purpose at this point because, as alleged, their personal information was already sold and is available on the dark web." *Id*. at 780. Thus, the court concluded the plaintiffs "failed to allege a future harm caused by the unfair practice, as required by the GUDTPA." *Id*. Here, as in *Collins*, an injunction will not remedy Baton's alleged injuries because they stem from the alleged disclosure of his contact information, which a Court order cannot undo. Further, Baton's allegation that he "remain[s] at imminent risk that further compromises of [his] personal information will occur in the future," and that "the risk of another [data breach] is real, immediate, and substantial" (FAC ¶¶ 187, 190) are hypothetical future harms, predicated on the potential actions of unknown third parties, that do not entitle him to relief under the GUDTPA. *See*, *infra*, Section IV.D(1); *see also Byung Ho Cheoun v. Infinite Energy, Inc.*, 363 F. App'x 691, 695 (11th Cir. 2010) (affirming dismissal of GUDTPA claim when plaintiffs only alleged hypothetical future harm).

5. Plaintiff Comilla's New York GBL §§ 349 and 350 claims fail

To assert claims under GBL §§ 349 and 350, "a plaintiff must allege that a defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice." *Orlander v. Staples, Inc.*, 802 F.3d 289, 300 (2d Cir. 2015) (internal citations omitted). A statement is actionable under §§ 349 and 350 only if it is "likely to mislead a reasonable consumer acting reasonably under the circumstances." *Maurizio v. Goldsmith*, 230 F.3d 518, 521 (2d Cir. 2000). "It is well settled that a court may determine as a matter of law that an allegedly deceptive [statement] would not have misled a reasonable consumer." *Fink v. Time Warner Cable*, 714 F.3d 739, 741 (2d Cir. 2013).

Plaintiff Comilla does not allege facts showing that reasonable consumers interpreted Ledger's Privacy Policy and statements about the security of the hardware wallets to mean consumers' "personal data… will remain anonymous, secure and private." (FAC ¶ 6; *see, supra* Section IV.C(1)(a).) *Abdale* is instructive. There, plaintiffs alleged their personal information was disclosed in a data breach. *Abdale v. N. Shore-Long Island Jewish Health Sys., Inc.*, 19

N.Y.S.3d 850, 859 (N.Y. Sup. Ct. 2015). The plaintiffs alleged the defendants violated GBL 349 because the defendants' privacy policy "guarantee[d] that plaintiffs' protected health information would not be released to any unauthorized third parties." *Id.* The court disagreed, finding "the statements allegedly made by defendants in the privacy policy and online notices do not constitute an unlimited guaranty that patient information could not be stolen or that computerized data could not be hacked." *Id.* at 859. Therefore, the defendants' alleged failure to safeguard the plaintiffs' personal information "did not misled the plaintiffs in any material way" and "does not constitute a deceptive practice" under section 349. *Id.* at 860. Here, like in *Abdale*, Ledger's Privacy Policy did not guarantee that Comilla's contact information would be completely secure. (FAC ¶ 6.) In fact, as Comilla acknowledges, the policy expressed provides "the transmission of information on the Internet is not fully secure." (*Id.*)

Nor does Comilla state a claim based on Ledger's alleged failure to disclose that "it did not reasonably or adequately secure" or "comply with common law and statutory duties pertaining to the security and privacy of" his contact information. (FAC ¶¶ 274-75.) Omission-based claims under §§ 349 and 350 are appropriate only "where the business alone possesses material information that is relevant to the consumer and fails to provide this information." *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A.*, 85 N.Y.2d 20, 26 (1995). Plaintiffs pursuing an omission-based claim must "plausibly allege that the defendants had knowledge of the material information and failed to disclose or actively concealed such information." *In re Sling Media Slingbox Advert. Litig.,* 202 F. Supp. 3d 352, 359 (S.D.N.Y. 2016) (internal citations omitted). Comilla does not allege that Ledger was aware of any security vulnerabilities in its e-commerce database. Without knowledge, there can be no omissions.

6. Plaintiffs' requests for equitable relief must be dismissed because they do not allege they lack an adequate remedy at law

Plaintiffs' UCL claim must be dismissed in its entirety under *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 841 (9th Cir. 2020), because the UCL provides exclusively equitable relief, and Plaintiffs do not and cannot establish that they lack an adequate remedy at law. *See* Cal. Bus. & Prof. Code § 17203 (UCL remedies); *Chowning v. Kohl's Dep't Stores, Inc.*, No. CV 15-08673

RGK (SPx), 2016 WL 1072129, at *5 (C.D. Cal. Mar. 15, 2016) ("[D]amages . . . are not available under the UCL" (quoting *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1148 (2003) (alteration in original).) *Sonner* also requires dismissal of Plaintiffs' CLRA, declaratory judgment and injunctive relief, GUDTPA, GFBPA, and New York GBL §§ 349 and 350 claims to the extent they seek equitable relief, including injunctive relief. (FAC ¶¶ 189 259, 270, 276); *see, e.g.*, *In re MacBook Keyboard Litig.*, No. 5:18-cv-02813-EJD, 2020 WL 6047253, at *3 (N.D. Cal. Oct. 13, 2020) ("[N]othing about the Ninth Circuit's reasoning [in *Sonner*] indicates that the decision is limited to claims for restitution. In fact, numerous courts in this circuit have applied *Sonner* to injunctive relief claims.")

Sonner concluded that notwithstanding what state law may permit, the Supreme Court has consistently made clear that federal courts are bound by the "rigid restrictions" on their equitable powers explicitly enumerated in *Guaranty Trust Co. of New York v. York*, including the requisite inadequacy of legal remedies. *Sonner,* 971 F.3d at 842 (citing *Guaranty Tr. Co. of N.Y. v. York*, 326 U.S. 99, 105-06 (1945)). Thus, traditional federal equitable principles, not state law, govern the determination whether to award equitable relief in a diversity action: "[S]tate law can neither broaden nor restrain a federal court's power to issue equitable relief." *Id.* at 841. Accordingly, *Sonner* affirmed dismissal of UCL and CLRA claims for equitable restitution because the plaintiff did not plead "the inadequacy of remedies at law" and sought money damages under the CLRA. *Id*. at 844 (quoting *O'Shea v. Littleton*, 414 U.S. 488, 502 (1974)).

Here, as in *Sonner,* Plaintiffs do not plead any facts showing "the inadequacy of remedies at law." Nor could they: Plaintiffs admit damages are a viable remedy and seek "compensatory, punitive, and nominal damages" including for the "theft of their personal information," "diminished value" of their hardware wallets, and the costs associated with the "detection and prevention of phishing scams [and] purchasing new hardware and software to protect crypto assets" for their negligence claim. (FAC ¶ 177.) They also seek damages for their negligence per se, CLRA, deceit by concealment, GFBPA, and New York GBL §§ 349 and 350 claims. (FAC ¶¶ 183, 237, 247, 270, 276.)

The Court need not accept Plaintiffs' conclusory allegations that "some damages (such as continuous risk of harm/identity theft/ongoing phising [sic] scams and other damages) cannot be remedied through a restitution, and injunctive relief would prevent some future harm – such as future misrepresentations and harm." (FAC ¶ 223.) Plaintiffs plead no facts showing any certainly impending injury that warrants injunctive relief. As established below, an injunction will not remedy their alleged injury of "continuous risk of harm/identity theft/ongoing phising [sic] scams." (*Id.*; *see, infra*, Section IV.D(1).) Their allegation of "some future harm" is also inadequate. (*Id.* ¶ 223.) Because Plaintiffs do not and cannot plead that they lack an adequate remedy at law, the Court should dismiss their UCL, CLRA, declaratory judgment and injunctive relief, GUDTPA, GFBPA, and New York GBL §§ 349 and 350 claims, for which they seek injunctive and equitable relief. *See In re MacBook Keyboard Litig.*, 2020 WL 6047253, at *4 (relying on *Sonner* and dismissing UCL and remaining claims "to the extent they seek an injunction, restitution, or other equitable relief").

7. Declaratory judgement and injunctive relief are not causes of action

Declaratory relief is "only a remedy" and "not an independent cause of action or theory of recovery." *Wishnev v. Nw. Mut. Life Ins. Co.*, 162 F. Supp. 3d 930, 952 (N.D. Cal. 2016); *see also Countrywide Home Loans, Inc., v. Mortg. Guar. Ins. Corp*., 642 F.3d 849, 852–53 (9th Cir. 2011)("[i]n passing the [Declaratory Judgment Act], Congress enlarged the range of remedies available in the federal courts but did not extend their jurisdiction") (internal citations omitted). The same is true for injunctive relief. *Owens v. Wells Fargo Bank, N.A.*, No. C 09-3354 PJH, 2009 WL 3353313, at *5 (N.D. Cal. 2009) ("Because a request for injunctive relief by itself does not state a cause of action, this claim is dismissed for failure to state a claim upon which relief may be granted."). In any event, as established below, even if injunctive relief was a cause of action, Plaintiffs lack standing to seek it. *See infra,* Section IV.D(1). Plaintiffs thus cannot allege a cause of action for declaratory judgment and injunctive relief, and the Court should dismiss this cause of action.

D. Plaintiffs Do Not Have Standing to Pursue Injunctive Relief and Plaintiff Seirafi Lacks Standing to Pursue Any Claim

A court must dismiss a plaintiff's claims under Rule 12(b)(1) if he does not have Article

III standing. *Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1122 (9th Cir. 2010). To establish Article III standing, a plaintiff must plead (1) an "injury in fact," (2) causation, and (3) redressability. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). Injury in fact requires "'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.*; *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). This injury also must be "fairly traceable" to the challenged conduct, and likely to be redressed by a favorable decision. *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141 (9th Cir. 2010) (quoting *Lujan*, 504 U.S. at 560). Plaintiff must himself have standing before he can represent a class, and "must allege and show that [he] personally [has] been injured, not that injury has been suffered by other, unidentified members of the class to which [he] belong[s]." *Spokeo*, 136 S. Ct. at 1547 n.6; *see also Warth v. Seldin*, 422 U.S. 490, 501 (1975).

1. Plaintiffs lack standing to seek injunctive relief

To seek injunctive relief, Plaintiffs "must demonstrate that [they are] 'realistically threatened by a *repetition* of the violation.'" *Gest v. Bradbury*, 443 F.3d 1177, 1181 (9th Cir. 2006). The "threatened injury must be *certainly impending* to constitute injury in fact, and allegations of possible future injury are not sufficient.'" *Id.* (quoting *Clapper v. Amnesty Int'l USA 1138*, 133 S. Ct. at 1141 (2013)). Injunctive relief will not redress Plaintiffs' alleged injuries, which they assert arise out of security incidents that already occurred. Nor do Plaintiffs allege facts showing that there is a real and immediate threat that cyber-criminals will hack Ledger or that other rogue Shopify employees will steal Ledger customer information again.

Injunctive Relief Will Not Remedy Alleged Past Harms. An order mandating that Ledger adopt certain digital security measures "will not provide any relief for past injuries or injuries incurred in the future because of a data breach that has already occurred." *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *8 (S.D. Cal. Nov. 3, 2016) (injunction will not redress plaintiff's injuries arising from previous data breach). All of Plaintiffs' purported injuries stem from the past disclosure of their contact information. (FAC ¶¶ 96, 99, 100, 111, 118, 128, 140, 144.) Because no injunction will undo this disclosure, Plaintiffs lack standing to seek injunctive relief. *See Collins*, 356 Ga. App. at 780 (finding "an injunction would serve no purpose" where plaintiffs alleged "their personal information was already sold and is available on the dark web").

There Is No Imminent Risk of Future Injury. Plaintiffs are also not entitled to injunctive relief based on their "allegations of possible future injury." *Gest*, 443 F.3d at 1181. They do not allege facts showing that a cyber attack on Ledger's e-commerce database is "certainly impending." *Clapper*, 133 S. Ct. at 1141. Rather, they generally allege they "remain at imminent risk that further compromises of their personal information will occur in the future," and that "the risk of another [data breach] is real, immediate, and substantial." (FAC ¶¶ 187, 190.) This "fear [] of hypothetical future harm" is insufficient. *See Clapper*, 133 S. Ct. at 1151. These allegations are too speculative because the "future harm is based entirely on the decisions or capabilities of an independent, and unidentified, actor." *In re Zappos.com, Inc. Customer Data Sec. Breach Litig.*, 108 F. Supp. 3d 949, 959 (D. Nev. 2015) (citing *Clapper*, 133 S. Ct. at 1150); *see also Willingham*, 2013 WL 440702, at *6, 17 (plaintiffs lacked standing where alleged future risk of harm was "'dependent on entirely speculative, future actions of an unknown third-party'").

2. Plaintiff Seirafi lacks Article III standing

Plaintiff Seirafi does not plead injury in fact. He cannot establish standing based on the alleged disclosure or use of his contact information, unspecified emotional distress, economic injury, or risk of future harm.[15]

No Standing Based on Disclosure of Contact Information. Seirafi does not allege the disclosure of any sensitive personal information. The "sensitivity of the personal information, combined with its theft" are prerequisites to finding that Seirafi "adequately alleged an injury in fact." *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018); *Rahman v. Marriott Int'l, Inc.*, No. SA CV 20-00654-DOC-KES, 2021 WL 346421, at *2 (C.D. Cal. Jan. 12, 2021) (No injury when plaintiff does not allege his "sensitive data—such as credit card information, passports, or social security numbers—has fallen into the wrong hands."). "Without a hack of information such as social security numbers, account numbers, or credit card numbers, there is no obvious, credible risk of identity theft that risks real, immediate injury." *Antman v. Uber Techs., Inc.*, No. 15-cv-01175-LB, 2018 WL 2151231, at *9 (N.D. Cal. May 10, 2018) (disclosure of driver's license numbers and driver names did not establish an increased risk of injury); *Low v. LinkedIn Corp.,* No. 11-CV-01468-LHK, 2011 WL 5509848, at *6 (N.D. Cal. Nov. 11, 2011) (no injury where plaintiff did not allege "that his credit card number, address, and social security number have been stolen or published or that he is a likely target of identity theft as a result of [the data disclosure]."). The disclosed information—Seirafi's name, email address, phone number, and postal address—can be easily found on the internet or through public records.[16] In fact, the information is so innocuous that California's data breach notification law did not require Ledger to notify Seirafi when it was disclosed (though Ledger did so). Cal. Civ. Code § 1798.82.

---

[15] If this case proceeds past the pleading stage, it is unlikely that the other Plaintiffs will be able to prove standing.

No Standing Based on Alleged Use of Disclosed Contact Information. Seirafi does not allege that the cyber criminals used his contact information to commit identity theft or that he has lost a single cent because of the data breach. Nor does he allege that he has been the victim of a "SIM-swap" attack or lost money or crypto assets due to phishing emails or demands for payment. The fact that other Plaintiffs may have experienced these things does not help Seirafi establish standing because he "must allege a distinct and palpable injury to himself, even if it is an injury shared by a large class of other possible litigants." *Warth*, 422 U.S. at 501.

Seirafi also cannot establish standing based on the alleged fake 911 call by an unknown person that resulted in police being dispatched to his home because he does not plausibly allege it is "fairly traceable" to either the Ledger cyber attack or the Shopify incident. *See Lujan*, 504 U.S. at 560 ("the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party") (citations omitted). He fails to allege that either security incident—which occurred approximately eight months before the fake 911 call—caused the police to be called to his home. Nor does he provide any details plausibly linking the fake 911 call to either incident. Although unfortunate, the call does not establish Article III standing. *See also Novak v. United States*, 795 F.3d 1012, 1019 (9th Cir. 2015) (dismissing claim where the plaintiff alleged that third-parties "may well have engaged in the[] injury-inflicting actions"); *Oneto v. Ryland Grp., Inc*., No. EDCV 09-01670 VAP (DTBx), 2010 WL 11506425, at *8 (C.D. Cal. Mar. 31, 2010) (dismissing claim where plaintiffs had not pled a chain of causation between defendants' conduct and their harm).

---

[16] *See e.g.* https://www.fastpeoplesearch.com/naeem-seirafi_id_G6100017820194900856 (last visited July 26, 2021).

No Standing Based on Alleged Emotional Distress. Seirafi's conclusory allegations that he suffered unspecified emotional distress also do not establish injury-in-fact. "[A] plaintiff must support [his] claim for pain and suffering 'with something more than [his] own conclusory allegations,' such as specific claims of genuine injury." *Dewi v. Wells Fargo Bank*, No. CV 12-2891 ABC (SHx), 2012 WL 10423239, at *8-9 (C.D. Cal. Aug. 8, 2012) (quoting *Myers v. Bennett Law Offices*, 238 F. Supp. 2d 1196, 1206 (D. Nev. 2002)). Where, as here, Seirafi alleges "mental and emotional distress," but offers no specifics as to what mental and emotional distress he suffers from, he does not adequately allege injury. *See Sion v. SunRun, Inc*., No. 16-cv-05834-JST, 2017 WL 952953, at *2 (N.D. Cal. Mar. 13, 2017) (no injury when plaintiff generally alleges suffering "mental and emotional distress"). Seirafi's allegation that he was "frightened" by the fake 911 call, which happened while he was out of town, is not enough. (FAC ¶ 116.) Nor do anonymous posts on online message boards about the mental and emotional state of other people (some of whom say they do not live in the United States) help him establish standing because the Court can only consider the allegations pertaining to him.

No Standing Based on Purported Economic Injury. Seirafi's conclusion that he "paid an unwarranted premium" for the Ledger Nano X also does not confer standing. (FAC ¶ 210.) Courts reject this theory of injury when a plaintiff does not explain how the data breach affected the value of the goods he purchased. *See, e.g.*, *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949 at 961-62 (allegations that plaintiffs were harmed by an alleged decrease in the value of Zappos's services did not establish injury); *Jackson v. Loews Hotels, Inc.*, No. ED CV 18-827-DMG (JCx), 2019 WL 6721637, at *2 (C.D. Cal. July 24, 2019) (No injury when plaintiff "simply alleges that" funds for data security "were 'implied in the price paid'"). Here, Seirafi does not allege that the data breach affected the digital security of his Ledger Nano X or its value. Nor can he. His Ledger Nano X remains secure, and his allegation that the exposure of "the location of the purchased Ledger Products… inherently impacts the security of the Products" is implausible and directly contradicted by his other allegations. (FAC ¶ 141.) He admits the hardware wallet's location is irrelevant to its security. (*See id.* ¶¶ 48-49) (Ledger hardware wallets "do not 'hold' cryptocurrency in the way a traditional wallet stores cash. Rather, consumers store their private keys on these physical devices....The wallet itself can be accessed only by entering a PIN. Simply misplacing the wallet thus poses no risk of theft.") Because the data breach did not affect the digital security of Seirafi's Ledger Nano X or the cryptocurrency it controls, he cannot establish standing based on his purchase of the hardware wallet.

No Standing Based on Future Risk of Harm. Lacking any current injuries stemming from the data breach, Seirafi speculates that he is at *risk* of fraud due to increased phishing emails, "SIM-swap" attacks, and ransom threats. (*Id.* ¶¶ 96, 106, 115.) His allegation that the disclosure of his contact information "can lead" to injury is insufficient under the Supreme Court's decision in *Clapper*. (*Id.* ¶ 115.) In *Clapper*, plaintiffs who challenged government surveillance authority lacked standing because their alleged injury—interception of their communications—relied on an "attenuated chain of possibilities" and thus was not "certainly impending." *Clapper*, 133 S. Ct. at 1148. Like in *Clapper*, Seirafi asks this Court to speculate that the cyber criminals or other malfeasors who disclosed his contact information will select him from the "million other customers" whose contact information was disclosed (FAC ¶ 93), target him for fraud, that he will choose to reveal further personal information to the criminals, and that the information he discloses will be sufficient to commit fraud. Such an "attenuated chain" was insufficient in *Clapper*, and it is insufficient here. Therefore, Seirafi lacks Article III standing and his claims should be dismissed.

E. The Court Should Strike Plaintiffs' "Consumer" Class and Subclasses

In addition to eight other classes and subclasses, Plaintiffs seek to assert claims on behalf of a "Nationwide, UK, and Israel Consumer Class" and California, Georgia, and New York "Consumer Subclass[es]" comprising "all persons residing in [those locations] who purchased a [Ledger wallet] from Ledger or an authorized reseller within the limitations period, as may be extended or tolled by any applicable rule of law or equitable doctrine." These purported "consumer" classes have no nexus whatsoever to Plaintiffs' claims, which arise out of two security incidents, the Ledger cyber attack and the Shopify incident. The Court should strike these classes, which are unconnected to Plaintiffs' allegations, facially overbroad, and include individuals who have not been injured.

Rule 12(f) authorizes courts to strike "immaterial" and "impertinent" matters from the pleadings. Fed. R. Civ. P. 12(f). Courts may also order a party to amend the pleadings to remove class allegations under Rule 23(d)(1)(D). Fed. R. Civ. P. 23(d)(1)(D). Courts strike class allegations when they are unrelated to a plaintiff's claims. *Sandoval v. Ali*, 34 F. Supp. 3d 1031, 1044 (N.D. Cal. 2014) (striking class allegations inconsistent with plaintiffs' theory of the case). And, because "no class may be certified that contains members lacking Article III standing[,]" *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 594 (9th Cir. 2012) (internal citation omitted), courts strike class allegations where, as here, class members have not been injured. *Hovsepian v. Apple, Inc.*, No. 08-5788 JF (PVT), 2009 WL 5069144, at *6 (N.D. Cal. Dec. 17, 2009) (striking class allegations when proposed class members could not have experienced alleged harm).

Sandoval is instructive. There, the plaintiffs alleged the defendants used an unlawful piece rate method to pay employees in violation of the Fair Labor Standards Act and sought to represent all non-exempt employees. *Sandoval*, 34 F. Supp. 3d at 1038. The proposed class included individuals who were not paid according to the piece rate system at issue. *Id*. Because the class was "inconsistent with [p]laintiffs' theory of the case," the court struck the class allegations as overbroad. *Id.* at 1044. Here, Plaintiffs' alleged "consumer" classes suffer from the same fatal defect. By definition, they include individuals who ***were not affected*** by the security incidents that underlie Plaintiffs' claims. (FAC ¶ 145.) For example, they include every person in the United States, United Kingdom, or Israel who purchased a Ledger wallet:

- From a reseller, and thus did not provide their contact information to Ledger;
- From Ledger before the security incidents, but whose contact information the criminals did not access; and
- From Ledger after the security incidents.

Further, because these individuals have used their Ledger wallets without issue, they lack standing. *See Sanders v. Apple Inc.*, 672 F. Supp. 2d 978, 989–90 (N.D. Cal. 2009) (striking allegations of proposed class that lacked standing). Thus, the Court should strike Plaintiffs' overbroad "consumer" class and subclasses, which are at odds with their theory of the case.

IV. CONCLUSION

For the reasons set forth above, Ledger respectfully requests that the Court dismiss the First Amended Complaint in its entirety.

Dated: July 26, 2021

MORRISON & FOERSTER LLP

By: */s/ Purvi G. Patel*
Purvi G. Patel

Attorneys for Specially Appearing Defendant Ledger SAS