UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

DENNIS NOWAK,
Plaintiff,
v.
XAPO, INC., et al.,
Defendants.

Case No. 5:20-cv-03643-BLF

ORDER GRANTING DEFENDANT'S MOTION TO DISMISS WITH LEAVE TO AMEND

[Re: ECF 22]

Dennis Nowak ("Plaintiff") sues Xapo, Inc., Xapo (Gibraltar) Limited, Indodax, and ten unidentified John Doe defendants (collectively, "Defendants") for hacking into his cryptocurrency exchange account, stealing 500 Bitcoins, and depositing them into separate hot wallet addresses. Plaintiff asserts violations of (1) California Penal Code § 496 (Possession of Stolen Property); (2) Aiding and Abetting under 18 U.S.C. § 1030(a)(4) (the Computer Fraud and Abuse Act); and (3) Assisting Unlawful Access to a Computer under California Penal Code § 502 et seq. (the Comprehensive Computer Data Access and Fraud Act). See generally Compl., ECF 1. Xapo, Inc. ("Defendant") brings this Motion to Dismiss for failure to state a claim. See Mot. to Dismiss ("Mot."), ECF 22. The Court heard arguments for the Motion on November 12, 2020. Mot. Hr'g, ECF 45. For the reasons stated on the record and discussed below, the Motion is GRANTED WITH LEAVE TO AMEND.

I. BACKGROUND

A. Factual Allegations

In November 2018, unidentified hackers infiltrated Plaintiff's account at a California cryptocurrency exchange and stole approximately 500 Bitcoins. Compl. ¶¶ 16-18, 20. At the time, the digital currency was valued at $2.3 million. Compl. ¶ 19. Plaintiff promptly hired

United States District Court
Northern District of California

Dockets.Justia.com

investigative firm Kroll to locate the stolen cryptocurrency. Compl. ¶ 21. Kroll traced it to addresses owned by custodial cryptocurrency firms Indodax and "Xapo." Comp. ¶¶ 22-25, 34. An investigation by Kroll also concluded that Indodax and "Xapo" employ inadequate policies and procedures to prevent use of their services for malicious activity. See Compl. ¶¶ 33-44.

B. Procedural History

On June 1, 2020, Plaintiff filed the Complaint against Defendants. See generally Compl. Plaintiff is a German resident. Compl. ¶ 1. Defendant Xapo, Inc. is a Delaware corporation with its principal place of business in California. Compl. ¶ 2. Defendants Xapo (Gibraltar) Limited and Indodax are foreign corporations. Compl. ¶¶ 3, 5. And the ten John Doe defendants are a collection of unidentified hackers. Compl. ¶ 6. On July 29, 2020, Defendant filed this Motion. See generally Mot. Plaintiff filed his Opposition on August 12, 2020. See generally Opp'n to Mot. to Dismiss ("Opp."), ECF 26. On August 19, 2020, Defendant filed its Reply. Reply in Supp. of Mot. to Dismiss ("Reply"), ECF 28. This Court held a hearing on November 12, 2020. Mot. Hr'g.

II. LEGAL STANDARD

A. Federal Rule of Civil Procedure 12(b)(6): Failure to State a Claim

"A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted 'tests the legal sufficiency of a claim.'" Conservation Force v. Salazar, 646 F.3d 1240, 1241-42 (9th Cir. 2011) (quoting Navarro v. Block, 250 F.3d 729, 732 (9th Cir. 2001)). When considering such a motion, the Court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." Manzarek v. St. Paul Fire & Marine Ins. Co., 519 F.3d 1025, 1031 (9th Cir. 2008). While a complaint typically need not contain detailed factual allegations, it "must contain sufficient factual matter, accepted as true, to 'state 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)). A claim is facially plausible when it "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." Id.

United States District Court
Northern District of California

B. Federal Rule of Civil Procedure 15(a): Leave to Amend

Under Federal Rule of Civil Procedure 15(a), the Court should freely grant leave to amend "when justice so requires," keeping in mind Rule 15's underlying purpose "to facilitate decision on the merits, rather than on the pleadings or technicalities." Lopez v. Smith, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (internal quotation marks and alterations omitted). When dismissing a complaint for failure to state a claim, "a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts." Id. at 1130 (internal quotation marks omitted).

III. DISCUSSION

Defendant raises numerous arguments in favor of dismissing the Complaint. These mostly center on Plaintiff's failure to plead sufficient facts showing actionable conduct, knowledge, or loss. See generally Mot. For the reasons discussed below, this Court largely agrees.

A. Notice Requirements of Rule 8(a)(2)

"[A] complaint which lumps together multiple defendants in one broad allegation fails to satisfy the notice requirement of Rule 8(a)(2)." Adobe Sys. Inc. v. Blue Source Grp., Inc., 125 F. Supp. 3d 945, 964 (N.D. Cal. 2015) (internal quotation marks and alterations omitted). Here, the Complaint lumps together defendants Xapo, Inc. and Xapo (Gibraltar) Limited, alleging conduct by "Xapo" without distinguishing what each entity did. Compl. ¶¶ 2-4. Xapo, Inc. and Xapo (Gibraltar) Limited are distinct corporations, the first domestic and the latter foreign. Compl. ¶¶ 2-3; Mot. 14-15; Reply 15. In an amended pleading, Plaintiff must identify exactly what action each took that caused his harm, without resorting to generalized allegations against "Xapo" (or "Defendants") as a whole.[1] See In re Nexus 6P Prod. Liab. Litig., 293 F. Supp. 3d 888, 907-08 (N.D. Cal. 2018) (requiring the plaintiff to distinguish each defendant's conduct).

B. California Penal Code § 496

In Count I, Plaintiff alleges violation of California Penal Code § 496 for possession of stolen property. Comp. ¶¶ 45-53. The elements are "(1) that the property has been stolen; (2) that

[1] Because the Complaint refers to "Xapo" throughout, this Order treats the facts alleged as if they are intended to apply to Xapo, Inc., who brought this Motion.

the accused received, concealed or withheld it from its owner; and (3) that the accused knew the property was stolen." People v. Stuart, 272 Cal. App. 2d 653, 656 (1969). The third element, "requires actual knowledge of or belief that the property is stolen." U.S. v. Flores, 901 F.3d 1150, 1161 (9th Cir. 2018) (citing People v. Tessman, 223 Cal. App. 4th 1293, 1302 (2014)).

Here, Plaintiff suggests that Defendant's knowledge can be inferred from its allegedly inadequate "Know Your Customer" ("KYC") and "Anti-Money-Laundering" ("AML") policies and procedures, claiming that, had Defendant followed reasonable compliance standards, it "knew or should have known" of the stolen property. Comp. ¶¶ 40-41, 51. Plaintiff argues that the extent of the inadequacy amounts to "willful blindness." Opp. 8-9; see also People v. Scaggs, 153 Cal. App. 2d 339, 352 (1957) ("[T]he requisite guilty knowledge can be inferred from circumstantial evidence."). But the Complaint fails to show how Defendant's KYC and AML policies and procedures amounted to the type of willful blindness contemplated by § 496, as opposed to mere negligence. See Freeney v. Bank of Am. Corp., No. CV 15-2376-JGB-PJWx, 2016 WL 5897773, at *11-12 (C.D. Cal. Aug. 4, 2016) (holding that the plaintiff failed to plead the bank's actual knowledge of converted funds despite being aware of several red flags).

Plaintiff further argues that even if Defendant was originally unaware of the theft, it became aware upon receiving notice of the Complaint. Opp. 9; see also Scaggs, 153 Cal. App. 2d at 352 (explaining that "even though a person is not aware that property is stolen when he first comes into possession of it, if he subsequently learns of its stolen nature and then conceals or withholds it from its true owner, he is guilty of a violation of [§] 496"). But filing a complaint itself is insufficient to prove actual knowledge under § 496. See Kidron v. Movie Acquisition Corp., 40 Cal. App. 4th 1571, 1586 (1995) (finding that service of the complaint gave the defendant notice of a claim for fraud, not actual knowledge of the fraud itself).

In sum, Plaintiff fails to plead sufficient facts demonstrating Defendant's knowledge that it came into possession of stolen funds. Thus, Defendant's Motion as to Count I is GRANTED WITH LEAVE TO AMEND.

C. The Computer Fraud and Abuse Act ("CFAA")

In Count II, Plaintiff alleges aiding and abetting under 18 U.S.C. § 1030(a)(4) of the

United States District Court
Northern District of California

CFAA. Compl. ¶¶ 54-61. To succeed, Plaintiff must show that Defendant "(1) accessed a protected computer, (2) without authorization or exceeding such authorization that was granted, (3) knowingly and with intent to defraud, and thereby (4) furthered the intended fraud and obtained anything of value." U.S. v. Nosal, 930 F. Supp. 2d 1051, 1058 (N.D. Cal. 2013) (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009)) (internal quotation marks and alterations omitted). Plaintiff's Complaint fails to state a claim for the reasons below.

1. Failure to Plead Facts with Specificity Under Rule 9(b)

Under Federal Rule of Civil Procedure 9(b), a party must, in alleging fraud or mistake, "state with particularity the circumstances constituting fraud or mistake." For CFAA claims, "Rule 9(b) plainly applies to § 1030(a)(4)'s requirement that the defendant's acts further the intended fraud." Oracle Am., Inc. v. Serv. Key, LLC, No. C 12-00790 SBA, 2012 WL 6019580, at *6 (N.D. Cal. Dec. 3, 2012). Here, Plaintiff alleges that Defendant assisted the unidentified hackers by providing them "safe havens" in its custodial vaults to hide the stolen Bitcoins and that Defendant "knew or should have known the property was so stolen or obtained." Compl. ¶¶ 59-60. To support these allegations, Plaintiff provides conclusory statements that investigative firm Kroll found Defendant's KYC and AML policies and procedures to be inadequate. See Compl. ¶¶ 33-42. The pleadings for Plaintiff's CFAA claim "should include the 'who, what, when, where, and how of the misconduct charged.'" In re Apple Inc. Device Performance Litig., 386 F. Supp. 3d 1155, 1181 (N.D. Cal. 2019) (quoting Kearns v. Ford Motor Co., 567 F.3d 1120, 1124 (9th Cir. 2009)). Thus, the Complaint suffers for lack of specificity in pleading the facts.

2. Failure to Allege the Requisite Conduct or Intent

The CFAA "was designed to target hacking, not misappropriation." Koninklijke Philips N.V. v. Elec-*Tech Int'l Co., Ltd.*, No. 14-cv-02737-BLF, 2015 WL 1289984, at *4 (N.D. Cal. Mar. 20, 2015) (citing U.S. v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012) (en banc)). As such, to violate the statute a party must "engage in the hacking, not merely benefit from its results." Id. Furthermore, the "intent to defraud" element requires "knowing and specific conduct." U.S. v. Nosal, 844 F.3d 1024, 1032-33 (9th Cir. 2016).

Here, Plaintiff fails to allege that Defendant actually engaged in any hacking or that

Defendant had the requisite knowledge of the hacking itself. See generally Compl. Instead, the Complaint alleges that Defendant had actual or constructive knowledge of its inadequate security systems, which enabled the hacking to occur. Compl. ¶¶ 33-42, 59-60. Such conduct appears beyond the scope of the CFAA, and Plaintiff does not cite any law to the contrary. See Opp. 5-6.

Plaintiff attempts to circumvent the fact that Defendant apparently did not participate in or know about the hacking by asserting an aiding and abetting theory of liability. See Compl. ¶¶ 55, 59. Defendant argues that the CFAA does not provide a civil cause of action for aiding and abetting. See Mot. 8-9; Reply 3, 7-8. Decisions on the issue are mixed. Compare COR Securities Holdings Inc. v. Banc of California, N.A. No. SA CV 17-1403-DOC (JCGx), 2018 WL 4860032, at *7 (C.D. Cal. Feb. 12, 2018) (finding that, in light of several recent Ninth Circuit decisions, the court was not persuaded "that legal precedent forecloses a civil aiding and abetting claim under [the] CFAA") and Tracfone Wireless, Inc. v. Simply Wireless, Inc., 229 F. Supp. 3d 1284, 1296-97 (S.D. Fla. 2017) (finding that a civil "defendant can be held liable under the CFAA under an aiding and abetting theory of liability") with Flynn v. Liner Grode Stein Yankelevitz Sunshine Regenstreif & Taylor LLP, No. 3:09-CV-00422-PMP-RAM, 2011 WL 2847712, at *3 (D. Nev. July 15, 2011) (finding that "aiding and abetting civil liability does not exist under § 1030") and Advanced Fluid Sys., Inc. v. Huber, 28 F. Supp. 3d 306, 328 (M.D. Pa. 2014) (same).

But even if such liability exists, Plaintiff fails to allege facts demonstrating that Defendant aided and abetted the hacking. Plaintiff asserts instead that Defendant provided a "safe haven" for the stolen property in its custodial vaults. Compl. ¶ 59. But Plaintiff does not allege that Defendant substantially assisted in the hacking itself, the primary violation. See generally Compl.; see also Flynn, 2011 WL 2847712, at *3 (finding no aiding and abetting of the CFAA where the defendants were alleged merely to have received the hacked information and to have used it knowing its illicit source) (citing Ponce v. S.E.C., 345 F.3d 722, 737 (9th Cir. 2003)). Instead, the CFAA claim appears to rely only on Defendant's alleged acts or omissions after the hacking occurred. See generally Compl.

Thus, the Complaint fails to allege conduct or knowledge, whether direct or indirect, giving rise to liability under the CFAA.

United States District Court
Northern District of California

3. Failure to Allege a Cognizable "Loss"

The CFAA provides a civil remedy for "[a]ny person who suffers damage or loss by reason of a violation of this section." 18 U.S.C. § 1030(g). "Damage" is "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). A "loss" is "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C.§ 1030(e)(11). Additionally, a civil action for violating § 1030(a)(4) may be brought only if the conduct caused a "loss to one or more persons during any one-year period aggregating at least $5,000 in value." Brekka, 581 F.3d at 1132; 18 U.S.C. § 1030(c)(4)(A)(i)(I). Courts have interpreted "loss" to mean "the types of costs . . . related to fixing a computer." Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 475 (S.D.N.Y. 2004), *aff'd*, 166 F. Appx. 559 (2d Cir. 2006); see also Delacruz v. State Bar of Cal., No. 16-cv-06858-BLF, 2018 WL 3077750, at *8 (N.D. Cal. Mar. 12, 2018), *aff'd*, 768 F. Appx. 632 (9th Cir. 2019).

Here, Plaintiff alleges that he suffered the loss of the value of his 500 Bitcoins. See Compl. ¶¶ 18-32; Opp. 7. But losing the value of his stolen cryptocurrency is not a cognizable loss under the CFAA. See DCR Mktg., Inc. v. Pereira, No. 19-CV-3249 (JPO), 2020 WL 91495, at *2-3 (S.D.N.Y. Jan. 8, 2020) (finding that funds wrongfully transferred from the plaintiff's bank accounts were not cognizable losses under the CFAA); Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio, Civil No. 09-2751, 2010 WL 4224473, at *5-7 (E.D. Pa. Oct. 22, 2010) (same).

Additionally, Plaintiff claims in his Opposition that he incurred more than $5,000 in costs when he hired international investigative firm Kroll to trace his stolen Bitcoins. Opp. 7. While Plaintiff may amend his Complaint to incorporate facts demonstrating these costs, it is unclear how hiring an investigative firm to trace stolen funds constitutes a cognizable "loss" relating to computers under the CFAA. Se*e Tyco Int'l* (US) Inc. v. John Does 1-3, No. 01 Civ. 3856 RCCDF, 2003 WL 21638205, at *1-2 (S.D.N.Y. July 11, 2003) (finding that costs incurred by hiring an investigative firm to locate and gather information about an unidentified hacker were not

United States District Court
Northern District of California

cognizable under the CFAA); see also Nexans Wires S.A., 319 F. Supp. 2d at 475-76 (explaining what alleged conduct constitutes a "loss" under the CFAA).

In sum, Plaintiff has failed to state a claim under the CFAA. Accordingly, Defendant's Motion as to Count II is GRANTED WITH LEAVE TO AMEND.[2]

D. The Comprehensive Computer Data Access and Fraud Act ("CDAFA")[3]

In Count III, Plaintiff alleges violation of California Penal Code § 502 et seq. for assisting the unlawful access to a computer. Comp. ¶¶ 62-69. Although the Complaint does not state specifically which subsection of the CDAFA Defendant violated, it appears that Plaintiff is alleging violation of § 502(c)(6), which makes it unlawful to "[k]nowingly and without permission provide[] or assist[] in providing a means of accessing a computer, computer system, or computer network in violation of this section."

"The CDAFA is California's state-law analogue to the CFAA." Ticketmaster L.L.C. v. Prestige Ent. W., Inc., 315 F. Supp. 3d 1147, 1174 (C.D. Cal. 2018). While the CDAFA does not impose a minimum of $5,000 in damages, the rest of "the necessary elements of [§] 502 do not differ materially from the necessary elements of the CFAA." Brodsky v. Apple Inc., 445 F. Supp. 3d 110, 131 (N.D. Cal. 2020) (quoting Multiven, Inc. v. Cisco Sys., Inc., 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010)). Hence, the circumstances here suggest that the CDAFA claim fails for the same reasons that the CFAA claim does. See id. at 131 (finding the claims "rise or fall" together).

First, because Plaintiff's CDAFA claim "sound[s] in fraud," it is subject to Rule 9(b) pleading standards. See In re Apple Inc. Device Performance Litig., 386 F. Supp. 3d at 1181 (applying Rule 9(b)'s heightened pleading standards to the CFAA and CDAFA). Second, Plaintiff fails to allege that Defendant was involved in the hacking itself, directly or indirectly. See Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 863 (N.D. Cal. 2011) (finding that the alleged conduct of failing to provide a sufficiently secure computer system fell outside the scope of liability contemplated by § 502). Third, he fails to allege that Defendant had the requisite

[2] Because Plaintiff has leave to amend, this Court does not rule on the issue of supplemental jurisdiction. See Mot. 9-10; Reply 8-9.
[3] The CDAFA is also referred to as the California Computer Crime Law ("CCCL").

United States District Court
Northern District of California

knowledge to impose liability for assisting the hacking. See Spy Dialer, Inc. v. Reya LLC, No. ED CV 18-1178 FMO (SHKx), 2018 WL 3689554, at *1 (C.D. Cal. July 26, 2018) (dismissing for failure to show that the defendant intentionally accessed the plaintiff's computers). Finally, while the CDAFA does not impose the loss minimum that the CFAA does, the issue here is not the amount, but whether the nature of Plaintiff's loss is even cognizable under § 502. See Mot. 12-13; Opp. 12; Reply 12.

Thus, Defendant's Motion as to Count III is GRANTED WITH LEAVE TO AMEND.

E. Extraterritorial Reach of State-Law Claims

Finally, the Complaint alleges (1) that Plaintiff, a foreign resident, "maintained an account [holding his Bitcoins] at a Northern California-based cryptocurrency exchange," (2) that the account was infiltrated by hackers, and (3) that the stolen funds were traced to hot wallet addresses controlled by "Xapo." Comp. ¶¶ 1, 2, 16, 20, 24. It does not appear that these allegations show a sufficient nexus between California and Defendant's alleged wrongful conduct. See Ehret v. Uber Tech. Inc., 68 F. Supp. 3d 1121, 1129-33 (N.D. Cal. 2014) (holding that the alleged facts showed "a sufficient nexus between California and the misrepresentations which form the basis of Plaintiff's claims" because the misrepresentations at issue "emanated from California"); Warner v. Tinder Inc., 105 F. Supp. 3d 1083, 1096-97 (C.D. Cal. 2015) (dismissing a UCL claim for failure to show extraterritorial reach where the complaint did not adequately allege that the harm emanated from California); see also Sullivan v. Oracle Corp., 51 Cal. 4th 1191, 1206-09 (2011) (upholding California's strong presumption against the extraterritorial application of California law). In an amended pleading, Plaintiff should clarify the Court's extraterritorial reach over the state law claims.

IV. ORDER

For the foregoing reasons, IT IS HEREBY ORDERED that Defendant's Motion to Dismiss is GRANTED WITH LEAVE TO AMEND. Plaintiffs shall file an amended complaint **no later than Monday, December 21, 2020**.

Dated: November 20, 2020

BETH LABSON FREEMAN
United States District Judge

United States District Court
Northern District of California